frfФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»
(НИУ «БелГУ»)

ИНСТИТУТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ И ЕСТЕСТВЕННЫХ НАУК

КАФЕДРА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

РАЗРАБОТКА ИНФОКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ ГРУППЫ КОМПАНИЙ ODEBRECHT В РЕСПУБЛИКЕ АНГОЛА

Выпускная квалификационная работа
обучающегося по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи
очной формы обучения, группы 07001307
Укуахамба Ядмилде Авелино

Научный руководитель
канд. техн. наук,
доцент кафедры
Информационно-телекоммуникационных систем и технологий
НИУ «БелГУ» Девицына С.Н

Рецензент
Ведущий инженер электросвязи Участка систем коммутации №1 г.Белгород Белгородского филиала
ПАО «Ростелеком» Уманец С.В.

БЕЛГОРОД 2017

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
(НИУ «БелГУ»)
ИНСТИТУТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ И ЕСТЕСТВЕННЫХНАУК
КАФЕДРА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ
Направление подготовки *11.03.02 Инфокоммуникационные технологии и системы связи*
Профиль *«Сети связи и системы коммутации»*

Утверждаю
Зав. кафедрой
«____» _____ 201_г.

ЗАДАНИЕ
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ

_____ Укуахамба Ядмилде Авелино _____

1. Тема ВКР «Разработка инфокоммуникационной инфраструктуры группы компаний Odebrecht в Республике Ангола»

Утверждена приказом по университету от «____» _____ 201_ г. № _____

2. Срок сдачи студентом законченной работы _____

3. Исходные данные к работе:
количество абонентов - 1464
количество офисов – филиалов компании – 6.

4. Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов):
4.1 Анализ существующей сети связи ГК Odebrecht
4.2 Обзор сетевых технологий
4.3 Разработка мультисервисной сети связи в центральном офисе г. Луанда
4.4 Разработка транспортного сегмента сети
4.5 Разработка рекомендаций по реализации инфокоммуникационной инфраструктуры ГК Odebrecht
4.6 Технико-экономическое обоснование проекта

5. Перечень графического материала (с точным указанием обязательных чертежей)
5.1 Проектируемая схема организации связи в Центральном офисе г. Луанда (А1, лист 1)
5.2 Проектируемая схема организации транспортной сети (А1, лист 1)
5.3 Ситуационная схема трассы прокладки кабеля и линейно-кабельных сооружений (А1, лист 1)
5.4 Проектируемая схема размещения оборудования (А1, лист 1)
5.5 Технико-экономические показатели проекта.

6. Консультанты по работе с указанием относящихся к ним разделов работы

Раздел	Консультант	Подпись, дата	
		Задание выдал	Задание принял
4.1 – 4.5	*канд. техн наук, Доцент. каф. ИТСиТ Девицына С.Н.*		
4.6	*канд. техн наук, Доцент. каф. ИТСиТ Болдышев А.В.*		

7. Дата выдачи задания _____

Руководитель
Кандидат технических наук, Доцент
кафедры Информационно-телекоммуникационных
систем и технологий»
НИУ «БелГУ» _____ *Девицына С.Н.*
(подпись)

Задание принял к исполнению _____*Укуахамба Я.А.*
(подпись)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Развитие и положение на рынке любой современной компании зависит от того, как налажен информационный обмен. Внедрение современных инфокоммуникационных технологий позволяет крупным фирмам эффективно управлять сетью филиалов, защищать коммерческую информацию, активно взаимодействовать с организациями-партнёрами. В Республике Ангола бурно развивающимися отраслями экономики страны являются нефтегазовая промышленность и строительство. Одним из лидеров в данном сегменте экономики является группа компаний Odebrecht. Любая крупная компания нуждается в современной инфокоммуникационной инфраструктуре. Защищённый обмен коммерческой информацией – одно из главных условий успешного ведения бизнеса. На сегодняшний день не во всех филиалах компании в Анголе существуют и эксплуатируются собственные телекоммуникационные системы. В большинстве случаев компания пользуется услугами связи, предоставляемыми оператором Ангола-Телеком. Это не всегда выгодно, так как объём передаваемой информации растёт, вместе с этим процессом растут расходы компании. На текущий момент филиалы для обеспечения производственных процессов остро нуждаются в современной инфокоммуникационной инфраструктуре, следовательно, тема ВКР является актуальной.

Основной целью проекта является обеспечение качественного и защищённого информационного обмена между филиалами ГК Odebrecht в Республике Ангола для улучшения взаимодействия между объектами компании и улучшения условий труда сотрудников.

Таким образом, требуется спроектировать территориально-распределённую сеть связи для 1464 абонентов, с учётом возможности взаимодействия филиалов друг с другом и оптимизации затрат на услуги связи.

1 АНАЛИЗ СУЩЕСТВУЮЩЕЙ СЕТИ СВЯЗИ ГРУППЫ КОМПАНИЙ ODEBRECHT

1.1 Описание ГК Odebrecht

Компания Odebrecht основана в Сальвадоре, Баия в Бразилии в 1944 году. Odebrecht стал многонациональной ведущей организацией в нескольких мировых экономических секторах. Odebrecht присутствует в 21 стране мира на 4 континентах и действует в 14 областях бизнеса, таких как машиностроение и строительство, нефть и газ, охрана окружающей среды, химическая и нефтехимическая промышленность, производство сахара и этанола, инвестиции, оборона и технологии, а также транспорт и логистика. На протяжении всей своей истории, Odebrecht успешно завершила более 2 000 проектов в этих областях.

Подразделение компании Odebrecht C. A. в Республике Ангола отвечает за стратегические направления деятельности организации и за сохранение её единства. Цель Odebrecht C. A. направлена на повышение качества развития бизнеса, продвижение людей, предполагает стратегическую поддержку своим дочерним компаниям, через децентрализованную модель управления.

Стремление к устойчивости, инновационный характер ведения бизнеса, уважение к людям и окружающей среде, эти характеристики Odebrecht способствуют положительному развитию и тому, что в настоящий момент это одна из крупнейших бизнес-групп в сфере строительства в мире.

Odebrecht участвует в сообществах, различных проектах, способствующих продвижение ценностей образования, развития, возможностей для создания рабочих мест, при уважении традиций и местных обычаев.

Зоны присутствия компании в мире показаны на рисунке 1.1.

Рисунок 1.1 – Глобальное Присутствие Odebrech

Филиалы компании располагаются в странах: Германия, Австрия, Гана, Объединенные Арабские Эмираты, Мозамбик, Португалия, США, Мексика, Гватемала, Колумбия, Эквадор, Парагвай, Перу, **Ангола**, Бразилия, Венесуэла, Доминиканская Республика, Панама, Куба, Аргентина. В компании работают более 24000 сотрудников.

[1]

1.2 Odebrech в Анголе

Odebrecht работает на рынке Анголы в области проектирования и строительства с 1984 года, компания была организована для выполнения крупных строительных инфраструктурных проектов, таких как дамб, систем водоснабжения и канализации, дорог, электросетей и недвижимости предприятий, которые внесли значительный вклад в развитие страны. Деятельность Odebrecht имеет цель поддержания безопасности рабочих проектов, в том числе в сфере охраны окружающей среды и производства качественных работ.

Все строительные работы, осуществляемые Odebrecht, сопровождаются социальными программами, разработанными с местными общинами, действуют образовательные программы, направленные на борьбу с неграмотностью населения, программы в области здравоохранения и целый ряд других социальных программ.

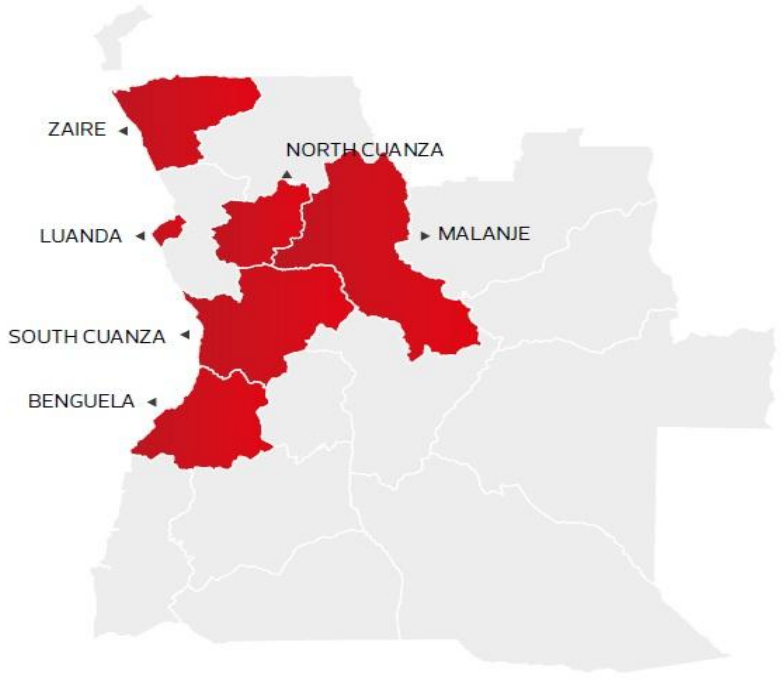

Рисунок 1.2 – Зона присутствия компании Odebrech в Анголе

В то же время Odebrecht были сделаны инвестиции в нескольких областях за пределами его основной деятельности, на примере своего участия в торговой сети «Nossosuper», в ЗАО «Биоком», а также в торговых сетях «Belas».

Компания Odebretcht в Анголе присутствует в 6 провинциях, и имеет более 1400 работников. Главный офис находится в провинции Луанда, который является столицей Республики Ангола.

[1, 2]

1.3 Постановка задачи проектирования

Любая крупная компания нуждается в современной инфокоммуникационной инфраструктуре. Защищённый обмен коммерческой информацией – одно из главных условий успешного ведения бизнеса.

На сегодняшний день не во всех филиалах компании в Анголе существуют и эксплуатируются собственные телекоммуникационные системы. В большинстве случаев компания пользуется услугами связи, предоставляемыми оператором Ангола-Телеком. Это не всегда выгодно, так как объём передаваемой информации растёт, вместе с этим процессом растут расходы компании. На текущий момент филиалы для обеспечения производственных процессов остро нуждаются в современной инфокоммуникационной инфраструктуре, следовательно, тема ВКР является актуальной.

Основной целью проекта является обеспечение качественного и защищённого информационного обмена между филиалами ГК Odebrecht в Республике Ангола для улучшения взаимодействия между объектами компании и улучшения условий труда сотрудников.

Таким образом, требуется спроектировать территориально-

распределённую сеть связи для 1464 абонентов, с учётом возможности взаимодействия филиалов друг с другом и оптимизации затрат на услуги связи.

Задачами проекта являются:

- Разработка мультисервисной сети связи в центральном офисе г.Луанда;

- Разработка транспортного сегмента сети,

- Разработка рекомендаций по реализации инфокоммуникационной инфраструктуры ГК Odebrecht;

- Технико-экономическое обоснование проекта.

2 ОБЗОР СЕТЕВЫХ ТЕХНОЛОГИЙ

2.1 Описание сетевых технологий для организации связи в филиалах

Для реализации инфокоммуникационной инфраструктуры филиалов компании чаще всего используют сетевые технологии, предполагающие обмен всеми видами информации на базе единой телекоммуникационной платформы.

Одним из лидеров при проектировании высокоскоросных надёжных сетей является технология Ethernet.

2.1.1 Технология Ethernet

Технология Ethernet развивалась поэтапно, от инструмента для реализации локальных сетей до уровня глобальных сетевых инфраструктур. Гибкость и масштабируемость, обход коллизий, полный дуплекс и гигабитные скорости – основные преимущества Ethernet. Широкий спектр экономически выгодных решений позволяет смело внедрять Ethernet как на магистралях, так и на сетях абонентского доступа.

Metro Ethernet строится по трехуровневой иерархической схеме и включает ядро, уровень агрегации и уровень доступа. Ядро сети строится на высокопроизводительных коммутаторах и обеспечивает высокоскоростную передачу трафика. Уровень агрегации также создается на коммутаторах и обеспечивает агрегацию подключений уровня доступа, реализацию сервисов и сбор статистики. В зависимости от масштаба сети, ядро и уровень агрегации могут быть объединены. Каналы между коммутаторами могут строиться на основе различных высокоскоростных технологий, чаще всего Gigabit Ethernet и 10Gigabit Ethernet. При этом

необходимо учитывать требования по восстановлению сети при сбое и структуру построения ядра. В ядре и на уровне агрегации обеспечивается резервирование компонентов коммутаторов, а также топологическое резервирование, что позволяет продолжать предоставление услуг при одиночных сбоях каналов и узлов. Существенного сокращения времени на восстановление можно добиться только за счет применения технологии канального уровня. Поддержка технологии EAPS — собственного протокола компании Extreme Networks, предназначеного для поддержки топологии, исключающей зацикливание трафика и ее перестроение в случае нарушений в кольцевых сетях Ethernet. Сети, использующие EAPS, обладают всеми положительным свойствами сетей SONET/SDH и Resilient Packet Ring (RPR) включая время восстановления топологии =50ms.

Уровень доступа строится по кольцевой или звездообразной схеме на коммутаторах Metro Ethernet для подключения корпоративных клиентов, офисных зданий, а также домашних и SOHO клиентов. На уровне доступа реализуется полный комплекс мер безопасности, обеспечивающих идентификацию и изоляцию клиентов, защиту инфраструктуры оператора.

Обзор технологии, виды Ethernet

Ethernet является пакетной технологией компьютерных сетей. Стандарты Ethernet определяют проводные соединения и электрические сигналы на физическом уровне, формат пакетов и протоколы управления доступом к среде – на канальном уровне модели OSI. Описание Ethernet приведено в перечне стандартов IEEE группы 802.3.

В качестве передающей среды в современных используют витую пару и оптический кабель. Метод управления доступом – множественный доступ с контролем несущей и обнаружением коллизий (CSMA/CD, Carrier Sense Multiply Access with Collision Detection), скорость передачи данных 10 Мбит/с, размер пакета от 72 до 1526 байт, описаны методы кодирования данных. Количество узлов в одном разделяемом сегменте сети ограничено

предельным значением в 1024 рабочих станции. Однако сеть, построенная на одном разделяемом сегменте, становится неэффективной задолго до достижения предельного значения количества узлов.

В зависимости от скорости передачи данных и передающей среды существует несколько вариантов технологии. Независимо от способа передачи стек сетевого протокола и программы работают одинаково практически во всех нижеперечисленных вариантах. Стандарт IEEE 802.3u Fast Ethernet обеспечивает обмен данными со скоростью 100 Мбит/с, стандарт IEEE 802.3z Gigabit Ethernet со скоростью 1000 Мбит/с. Реализована возможность работы в режиме полный дуплекс.

Большинство Ethernet-карт и других устройств имеет поддержку нескольких скоростей передачи данных, используя автоопределение скорости и дуплексности, для достижения наилучшего соединения между двумя устройствами. Если автоопределение не срабатывает, скорость подстраивается под партнёра, и включается режим полудуплексной передачи. Например, наличие в устройстве порта Ethernet 10/100 говорит о том, что через него можно работать по технологиям 10BASE-T и 100BASE-TX, а порт Ethernet 10/100/1000 – поддерживает стандарты 10BASE-T, 100BASE-TX, и 1000BASE-T.

Fast Ethernet

100BASE-T – стандарт 100 Мбит/с Ethernet, использующий в качестве среды передачи данных витую пару. Длина сегмента до 200-250 метров. Включает в себя 100BASE-TX, 100BASE-T4 и 100BASE-T2.

100BASE-TX, IEEE 802.3u – развитие технологии 10BASE-T, реализуется по топологии «звезда» на кабеле витая пара категории 5, в котором фактически используются 2 пары проводников, максимальная скорость передачи данных 100 Мбит/с.

100BASE-T4 – 100 МБит/с Ethernet по кабелю категории 3. Используют все 4 пары, в полудуплексном режиме.

Наиболее часто используемый стандарт в настоящее время – это 100BASE-FX – 100 Мбит/с Ethernet на основе волоконно-оптического кабеля. Максимальная длина сегмента 400 метров в полудуплексном режиме (для гарантированного обнаружения коллизий) или 2 километра в полнодуплексном режиме по многомодовому оптическому волокну, и до 32 километров по одномодовому.

Гигабит Ethernet

Стандарт Ethernet 1 Гбит/с – 1000BASE-T, IEEE 802.3ab . Используется экранированная витая пара категории 5e или категории 6. В передаче данных участвуют все 4 пары. Скорость передачи данных – 250 Мбит/с по одной паре.

1000Base-X – общий термин для обозначения технологии Гигабит Ethernet, использующей в качестве среды передачи данных оптоволоконный кабель, включает в себя 1000BASE-SX, 1000BASE-LX и 1000BASE-CX.

1000BASE-SX, IEEE 802.3z – 1 Гбит/с Ethernet технология, использует многомодовое волокно дальность прохождения сигнала без повторителя до 550 метров.

1000BASE-LX, IEEE 802.3z – 1 Гбит/с Ethernet технология, использует многомодовое волокно дальность прохождения сигнала без повторителя до 550 метров. Оптимизирована для дальних расстояний, при использовании одномодового волокна (до 10 километров).

1000BASE-LH (Long Haul) – 1 Гбит/с Ethernet технология, использует одномодовый оптический кабель, дальность прохождения сигнала без повторителя до 100 километров.

10 Гигабит Ethernet

Стандарт 10 Гигабит Ethernet включает в себя семь стандартов физической среды для LAN, MAN и WAN. В настоящее время описывается поправкой IEEE 802.3ae.

10GBASE-CX4 – Технология 10 Гигабит Ethernet для коротких

расстояний (до 15 метров), используется медный кабель CX4 и коннекторы InfiniBand.

10GBASE-SR – Технология 10 Гигабит Ethernet для коротких расстояний (до 26 или 82 метров, в зависимости от типа кабеля), используется многомодовое оптоволокно. Он также поддерживает расстояния до 300 метров с использованием нового многомодового оптоволокна (2000 МГц/км).

10GBASE-LX4 – использует уплотнение по длине волны для поддержки расстояний от 240 до 300 метров по многомодовому оптоволокну. Также поддерживает расстояния до 10 километров при использовании одномодового оптоволокна.

10GBASE-LR и 10GBASE-ER – эти стандарты поддерживают расстояния до 10 и 40 километров соответственно.

10GBASE-SW, 10GBASE-LW и 10GBASE-EW – эти стандарты используют физический интерфейс, совместимый по скорости и формату данных с интерфейсом OC-192 / STM-64 SONET/SDH. Они подобны стандартам 10GBASE-SR, 10GBASE-LR и 10GBASE-ER соответственно, так как используют те же самые типы кабелей и расстояния передачи.

10GBASE-T, IEEE 802.3an-2006 использует экранированную витую пару. Расстояния – до 100 метров.

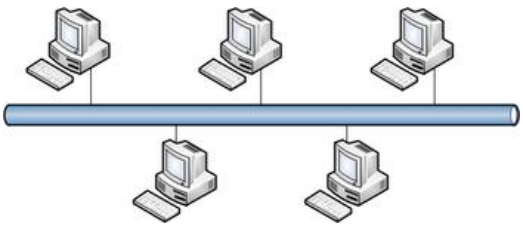

Рисунок 2.1 - Технология Ethernet

2.1.2 Технология Wi-Fi IEEE 802.11

Для реализации беспроводного сегмента рекомендуют использовать

технологию Wi-Fi. Технология Wi-Fi – беспроводной аналог стандарта Ethernet, на основе которого сегодня построена большая часть офисных компьютерных сетей.

Wi-Fi – сокращение от английского Wireless Fidelity, обозначающее стандарт беспроводной (радио) связи, который объединяет несколько протоколов и имеет официальное наименование IEEE 802.11. Чаще всего для реализации сетей используется протокол IEEE 802.11b, определяющий функционирование беспроводных сетей, в которых для передачи данных используется диапазон частот от 2,4 до 2,4835 ГГц и обеспечивается максимальная скорость 11 Мбит/сек. Максимальная дальность передачи сигнала в такой сети составляет 100 метров, однако на открытой местности она может достигать и больших значений (до 300-400 м).

В группе Wi-Fi присутствует версия 802.11a, использующая частоту 5 ГГц и обеспечивающая максимальную скорость 54 Мбит/с, а также 802.11g, работающая на частоте 2,4 ГГц, 54 Мбит/с. Новая версия стандарта 802.11n может обеспечить скорости до 320 Мбит/с.

Сеть Wi-Fi обеспечивает доступ к серверам, хранящим базы данных или программные приложения, на ее основе строят сегменты сетей абонентского доступа в Интернет. Компьютер или ноутбук размещается в радиусе трёхсот метров от точки доступа (access point) – Wi-Fi-устройства, выполняющего примерно те же функции, что обычная офисная АТС. В этом случае информация будет передаваться посредством радиоволн в частотном диапазоне 2,4-2,483 ГГц.

Таким образом, Wi-Fi-технология позволяет решить три важных задачи:

- упростить общение с мобильным компьютером;
- обеспечить комфортные условия для работы деловым партнерам, пришедшим в офис со своим ноутбуком,
- создать локальную сеть в помещениях, где прокладка кабеля

невозможна или чрезмерно дорога.

Кроме этого, использование сети Wi-Fi формирует корпоративный имидж и улучшает условия труда сотрудников. Поэтому принято решение в проекте использовать данную технологию в зданиях филиалов компании, где нет возможности работать со стационарным устройством, а также в конференц-зале и зоне ресепшн. Беспроводная технология может стать как основой IT-системы компании, так и дополнением к уже существующей кабельной сети. Для создаваемой инфраструктуры будет использован комбинированный вариант – частичное применение Wi-Fi. При этом ядром беспроводной сети Wi-Fi станет точка доступа (Access Point), которая будет подключаться к сетевой инфраструктуре в виде Ethernet-сети и обеспечивать передачу радиосигнала. Точка доступа состоит из приёмника, передатчика, интерфейса для подключения к проводной сети и программного обеспечения для обработки данных. После подключения вокруг точки доступа образуется территория радиусом 50-100 метров (хот-спот или зона Wi-Fi), на которой можно пользоваться беспроводной сетью.

Для того чтобы подключиться к точке доступа, сотруднику компании необходимо воспользоваться ноутбуком или другим мобильным устройством, оснащенным Wi-Fi адаптером, и попасть в радиус действия беспроводной сети. Все действия по определению устройств и настройке сети большинством ОС производятся автоматически. Если пользователь попадает одновременно в несколько Wi-Fi зон, то происходит подключение к точке доступа, обеспечивающей самый мощный сигнал. Время от времени производится проверка наличия других точек доступа, и в случае, если сигнал от новой точки сильнее, устройство переподключается к ней, настраиваясь абсолютно прозрачно и незаметно для владельца.

Одним из главных достоинств Wi-Fi сети является возможность доступа в Интернет для всех её пользователей, которая обеспечивается либо прямым подключением точки доступа к интернет-каналу, либо

подключением к ней любого сервера, соединенного с Интернет. При этом мобильному пользователю не нужно ничего самостоятельно настраивать - достаточно запустить браузер и набрать адрес какого-либо интернет-сайта.

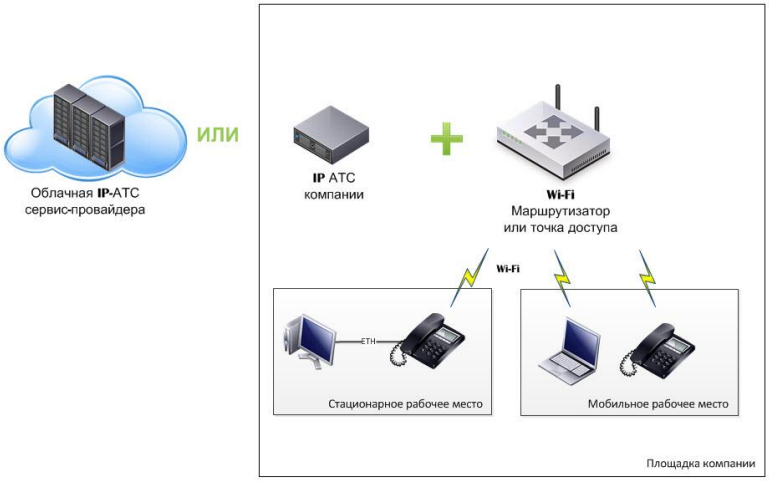

Рисунок 2.2 – Вариант применения технологии Wi-Fi в офисах компании Odebrecht

Также несколько устройств с поддержкой Wi-Fi могут соединяться друг с другом напрямую (связь устройство – устройство), то есть без использования специальной точки доступа, образуя некое подобие локальной сети, в которой можно обмениваться файлами, но в этом случае ограничивается число видимых станций.

Безопасность Wi-Fi

Для разрабатываемой корпоративной системы одним из важнейших условий ее функционирования является обеспечение информационной безопасности. Сети Wi-Fi являются уязвимыми, т.к. в беспроводной сети несанкционированный доступ можно осуществить гораздо проще, достаточно оказаться в зоне распространения радиоволн этой сети, даже вне здания офиса.

Любое взаимодействие точки доступа (сети), и беспроводного клиента, построено на:

- Аутентификации – как клиент и точка доступа представляются друг

другу и подтверждают, что у них есть право общаться между собой;

- Шифровании – какой алгоритм скремблирования передаваемых данных применяется, как генерируется ключ шифрования, и когда он меняется.

В стандарте 802.11 предусмотрены средства обеспечения безопасности, которые повышают защищенность беспроводной локальной сети до уровня обычно проводной локальной сети.

Способы шифрования в беспроводных сетях:

- **WEP** (WiredEquivalentPrivacy – секретность, эквивалентная проводной). Он представляет возможность шифровать данные, передаваемые через беспроводную среду, и тем самым обеспечивает их конфиденциальность;
- **WPA** (Wi-FiProtectedAccess – защищенный доступ к Wi-Fi) – более защищенный вариант беспроводных локальных сетей.
- **WPA2** – описывает надежное средство защиты беспроводных локальных сетей, сочетающее в себе наиболее совершенные средства аутентификации пользователей и шифрования данных. [2,4]

2.2 Выбор способа реализации транспортного сегмента

Для организации транспортной инфраструктуры на базе волоконно-оптических решений, используют различные технологии, предполагающие крупные инвестиции в сеть. Это не всегда оправдано, поэтому многие компании предпочитают использовать сети сторонних операторов, или провайдеров услуг. Одним из самых востребованных решений является VPN.

2.2.1 VPN – Виртуальные частные сети

Любая организация, будь она производственной, торговой, финансовой компании или государственным учреждением, обязательно сталкивается с вопросом передачи информации между своими филиалами, а также с вопросом защиты этой информации. Не каждая фирма может себе позволить иметь собственные физические каналы доступа, и здесь помогает технология VPN, на основе которой и соединяются все подразделения и филиалы, что обеспечивает достаточную гибкость и одновременно высокую безопасность сети, а также существенную экономию затрат.

Виртуальная частная сеть (VPN - Virtual Private Network) создается на базе общедоступной сети Интернет. И если связь через Интернет имеет свои недостатки, главным из которых является то, что она подвержена потенциальным нарушениям защиты и конфиденциальности, то VPN могут гарантировать, что направляемый через Интернет трафик так же защищен, как и передача внутри локальной сети. В тоже время виртуальные сети обеспечивают существенную экономию затрат по сравнению с содержанием собственной сети глобального масштаба.

Назанчение VPN

Главной отличительной чертой данной технологии является использование сети Internet в качестве магистрали для передачи корпоративного IP-трафика. Сети VPN предназначены для решения задач подключения конечного пользователя к удаленной сети и соединения нескольких локальных сетей. Структура VPN включает в себя каналы глобальной сети, защищенные протоколы и маршрутизаторы.

2.2.2 Принцип работы сети VPN

VPN-устройство располагается между внутренней сетью и Интернет на каждом конце соединения. Когда данные передаются через VPN, они исчезают «с поверхности» в точке отправки и вновь появляются только в точке назначения. Этот процесс принято называть «туннелированием». Это означает создание логического туннеля в сети Интернет, который соединяет две крайние точки. Благодаря туннелированию частная информация становится невидимой для других пользователей Интернета. Прежде чем попасть в интернет-туннель, данные шифруются, что обеспечивает их дополнительную защиту. Протоколы шифрования бывают разные. Все зависит от того, какой протокол туннелирования поддерживается тем или иным VPN-решением. Еще одной важной характеристикой VPN-решений является диапазон поддерживаемых протоколов аутентификации. Большинство популярных продуктов работают со стандартами, основанными на использовании открытого ключа, такими как X.509. Это означает, что, усилив свою виртуальную частную сеть соответствующим протоколом аутентификации, вы сможете гарантировать, что доступ к вашим защищенным туннелям получат только известные вам люди.

Имея доступ в Интернет, любой пользователь может без проблем подключиться к сети офиса своей фирмы. Общедоступность данных совсем не означает их незащищенность. Система безопасности VPN - это механизм, который защищает всю корпоративную информацию от несанкционированного доступа. Прежде всего, информация передается в зашифрованном виде. Прочитать полученные данные может лишь обладатель ключа к шифру. Наиболее часто используемым алгоритмом кодирования является Triple DES, который обеспечивает тройное шифрование (168 разрядов) с использованием трех разных ключей.

Подтверждение подлинности включает в себя проверку целостности

данных и идентификацию пользователей, задействованных в VPN. Первая гарантирует, что данные дошли до адресата именно в том виде, в каком были посланы. Самые популярные алгоритмы проверки целостности данных - MD5 и SHA1. Далее система проверяет, не были ли изменены данные во время движения по сетям, по ошибке или злонамеренно. Таким образом, построение VPN предполагает создание защищенных от постороннего доступа туннелей между несколькими локальными сетями или удаленными пользователями.

Для построения VPN необходимо иметь на обоих концах линии связи программы шифрования, исходящего и дешифрования, входящего трафиков. Они могут работать как на специализированных аппаратных устройствах, так и на ПК с такими операционными системами как Windows, Linux или NetWare.

Управление доступом, аутентификация и шифрование - важнейшие элементы защищенного соединения.

2.2.3 Основы туннелирования

Туннелирование (tunneling), или инкапсуляция (encapsulation) – это способ передачи полезной информации через промежуточную сеть. Такой информацией могут быть кадры (или пакеты) другого протокола. При инкапсуляции кадр не передается в сгенерированном узлом-отправителем виде, а снабжается дополнительным заголовком, содержащим информацию о маршруте, позволяющую инкапсулированным пакетам проходить через промежуточную сеть (Internet). На конце туннеля кадры деинкапсулируются и передаются получателю.

Этот процесс (включающий инкапсуляцию и передачу пакетов) и есть туннелирование. Логический путь передвижения инкапсулированных пакетов в транзитной сети называется туннелем.

2.2.4 Протоколы

Протокол VPN определяет, каким образом система VPN взаимодействует с другими системами в Интернете, а также уровень защищенности трафика. Если организация Odebrecht будет использовать VPN только для внутреннего информационного обмена, вопрос о взаимодействии можно не рассматривать, т.к. будут использованы механизмы собственной безопасности. В проекте рассматривается территориально-распределенная инфраструктурап, включающая офисы в 6 провинциях Анголы, поэтому организация Odebrecht будет использовать VPN для соединения с другими организациями и офисами, и собственные протоколы безопасности уже не будут работать на сетевых сегментах. Внешние окружающие факторы могут оказывать большее влияние на безопасность системы, чем алгоритм шифрования. Протокол VPN оказывает влияние на общий уровень безопасности системы. Причиной этому является тот факт, что протокол VPN используется для обмена ключами шифрования между двумя конечными узлами. Если этот обмен не защищен, злоумышленник может перехватить ключи и затем расшифровать трафик.

В разрабатываемом проекте сети необходимо предусмотреть механизмы защиты. Для того чтобы разрабатываемая на базе оборудования и программного обеспечения от различных производителей VPN была защищена, необходимо использовать протокол Internet Protocol Security (IPSec). IPSec описывает все стандартные методы VPN. Этот протокол определяет методы идентификации при инициализации туннеля, методы шифрования, используемые конечными точками туннеля и механизмы обмена и управления ключами шифрования между этими точками. Из недостатков этого протокола можно отметить то, что он ориентирован на IP.

Другими протоколами построения VPN являются протоколы PPTP (Point-to-Point Tunneling Protocol), разработанный компаниями Ascend

Communications и 3Com, L2F (Layer-2 Forwarding) - компании Cisco Systems и L2TP (Layer-2 Tunneling Protocol), объединивший оба вышеназванных протокола. Однако эти протоколы, в отличие от IPSec, не являются полнофункциональными (например, PPTP не определяет метод шифрования). Совместно с IPSec используют протокол IKE (Internet Key Exchange), позволяющий обеспечить передачу информации по туннелю, исключая вмешательство извне. Этот протокол решает задачи безопасного управления и обмена криптографическими ключами между удаленными устройствами, в то время, как IPSec кодирует и подписывает пакеты. IKE автоматизирует процесс передачи ключей, используя механизм шифрования открытым ключом, для установления безопасного соединения. Помимо этого, IKE позволяет производить изменение ключа для уже установленного соединения, что значительно повышает конфиденциальность передаваемой информации.

Инкапсуляция – обеспечивает мультиплексирование нескольких транспортных протоколов по одному каналу. Протокол LCP – PPP задает гибкий LCP для установки, настройки и проверки канала связи. LCP обеспечивает согласование формата инкапсуляции, размера пакета, параметры установки и разрыва соединения, а также параметры аутентификации. В качестве протоколов аутентификации могут использоваться PAP, CHAP и др.;

Протоколы управления сетью предоставляют специфические конфигурационные параметры для соответствующих транспортных протоколов. Например, IPCP протокол управления IP.

Для формирования туннелей VPN используются протоколы PPTP, L2TP, IPsec, IP-IP.

Протокол PPTP позволяет инкапсулировать IP-, IPX- и NetBEUI-трафик в заголовки IP для передачи по IP-сети, например, Internet.

Протокол L2TP позволяет шифровать и передавать IP-трафик с

использованием любых протоколов, поддерживающих режим «точка-точка» доставки дейтаграмм. Например, к ним относятся протокол IP, ретрансляция кадров и асинхронный режим передачи (ATM).

Протокол IPsec позволяет шифровать и инкапсулировать полезную информацию протокола IP в заголовки IP для передачи по IP-сетям.

В протоколе IP-IP IP-дейтаграмма инкапсулируется с помощью дополнительного заголовка IP. Главное назначение IP-IP – туннелирование многоадресного трафика в частях сети, не поддерживающих многоадресную маршрутизацию.

Для технической реализации сети VPN ГК Odebrecht, кроме стандартного сетевого оборудования, понадобится шлюз VPN, выполняющий все функции по формированию туннелей, защите информации, контролю трафика, а нередко и функции централизованного управления. При выборе АТС для сети филиала нужно предусмотреть возможность технической реализации поддержки VPN.

На сегодняшний день VPN – это экономичное, надежное и общедоступное решение организации удаленного доступа. Каким бы ни было расстояние, VPN обеспечит соединение с любой точкой мира и сохранность передачи самых важных данных.

2.2.5 Достоинства VPN

Виртуальные частные сети имеют несколько преимуществ над традиционными частными сетями. Главные из них – экономичность, гибкость и удобство использования.

Экономичность. С помощью VPN-сетей ГК Odebrecht удастся ограничить количество серверов доступа, коммутируемых линий и других технических средств, которые необходимо внедрять, чтобы обеспечить удаленным пользователям доступ к своим корпоративным сетям. Кроме

того, виртуальные частные сети дают возможность удаленным пользователям обращаться к сетевым ресурсам ГК Odebrecht не по дорогим арендованным линиям, а через местную телефонную связь.

Особенно выгодны виртуальные частные сети в тех случаях, когда пользователи удалены на большие расстояния и поэтому арендованные линии обходятся очень дорого, а также когда таких пользователей много, в связи с чем потребуется большое количество арендованных линий. Если объем трафика в VPN-сети слишком большой, система не успеет зашифровывать и расшифровывать пакеты данных. Чтобы избежать возникновения таких узких мест, ГК Odebrecht вынуждена будет покупать дополнительное оборудование. При выборе технических средств будет учтён данный фактор.

Кроме того, из-за относительной новизны технологии VPN и сложности используемых средств безопасности, в компании необходимо ввести должность системный администратор для поддержки виртуальной сети.

2.2.6 Недостатки VPN

Проблемы защиты данных, недостаток надежности и производительности, а также отсутствие открытых стандартов затрудняют широкое распространение виртуальных частных сетей.

Защита. Для большинства технологий Internet вопросы обеспечения безопасности при передаче данных являются ключевыми. Главные проблемы заключаются в аутентификации пользователей с помощью паролей и защите зашифрованного VPN-канала (тоннеля). Кроме того, сетевые администраторы должны тщательно выбирать методы, которые помогут сотрудникам ГК Odebrecht получать доступ к виртуальным частным сетям.

Чтобы уменьшить расходы, связанные с безопасностью, эти полномочия можно передать провайдеру. Провайдеры поддерживают широкий набор различных схем шифрования и аутентификации. Например, пакет программ для аутентификации клиентов и шифрования на уровне сеанса; оборудование, устанавливаемое между маршрутизатором и глобальной сетью, которое выполняет шифрование, аутентификацию и сжатие данных.

Большинство поставщиков используют методы шифрования с 56-разрядным ключом, соответствующие стандарту DES. Такая длина ключа обеспечивает достаточно высокий уровень безопасности. Некоторые поставщики продуктов для виртуальных частных сетей предлагают шифрование с 112-разрядным ключом. Увеличение длины ключа снижает производительность, так как чем сложнее алгоритм шифрования, тем более интенсивной вычислительной обработки он требует.

2.3 Выбор сценария реализации VPN ГК Odebrecht

Чтобы выбрать вариант реализации сетей MPLS-VPN с учетом масштабирования, проанализированы различные модели VPN. Вначале рассмотрим ограничения, присущие оверлейной или наложенной модели, а затем посмотрим, какие преимущества по сравнению с ней дает одноранговая модель.

Оверлейная модель

Сервис-провайдер предоставляет корпоративному заказчику технологию соединений между его офисами и отделениями по частной WAN IP-сети. Для этого в каждой точке подключения нужно установить маршрутизатор и связать его по какому-либо IGP-протоко-лу маршрутизации по крайней мере с центральным маршрутизатором. В этом случае сервис-провайдер предоставляет корпоративному заказчику частную

сетевую магистраль (private network backbone).

Если транспортная сеть и магистральные коммутаторы действительно принадлежат корпорации, это значит, что она имеет настоящую частную сеть. Однако чаще всего транспортная сеть и, по крайней мере, часть магистральных коммутаторов принадлежат сервис-провайдеру и совместно используются несколькими корпоративными сетями. В этом случае каждая из этих корпоративных сетей является не настоящей, а виртуальной частной сетью (VPN). В сети VPN с коммутацией каналов маршрутизаторы, которые находятся в разных отделениях компании, связываются между собой либо по выделенным, либо по коммутируемым линиям. В любом случае роль магистрали будет чаще всего выполнять телефонная сеть общего доступа. Сети Frame Relay и ATM основаны на технологии коммутации каналов. В этом случае маршрутизаторы, находящиеся в отделениях компании-заказчика, связываются между собой с помощью виртуальных каналов. Эти виртуальные каналы, подобно реальным, поддерживают соединения типа «точка-точка».

Корпоративные маршрутизаторы могут поддерживать соединения «точка-точка» и с помощью средств 1Р-туннелирования, например, IPSec или GRE. В таких частных или виртуальных частных сетях задачи дизайна и функционирования магистральной топологии решает сама корпорация или сервис-провайдер (если в сети предоставляются услуги по управлению). Маршрутизаторы, установленные в отделениях корпорации, связываются с соседними маршрутизаторами по каналам «точка-точка». Обмен данными о маршрутизации происходит напрямую по этим каналам.

С точки зрения магистральной сети сервис-провайдера, передаваемая маршрутная информация представляет собой обычные данные, которые обрабатываются «прозрачно», то есть так же, как и все остальные. Со своей стороны, корпоративные маршрутизаторы не имеют ни знаний, ни средств контроля над маршрутизирующими функциями магистрали. Этот домен

относится к сфере, за которую отвечает сервис-провайдер.

В этом случае корпоративная IP-сеть является оверлейной, то есть «накладывается» поверх провайдерской магистрали. При этом корпоративную сеть можно рассматривать как сеть более высокого уровня, а магистраль – как сеть более низкого уровня. Обе сети существуют независимо друг от друга. Такой способ построения сети более высокого уровня поверх сети более низкого уровня называется оверлейной моделью.

Недостатки оверлейной модели

Чтобы добиться оптимальной маршрутизации в корпоративной сети, надстроенной поверх магистрали, корпоративная сеть должна иметь узловую структуру (meshed network). Это означает, что в каждом отделении корпорации должен устанавливаться маршрутизатор, соединенный с соседними маршрутизаторами, находящимися в других отделениях.

Если корпоративная сеть будет хотя бы частично отклоняться от узловой топологии (meshed), то возникнут случаи, когда трафик будет передаваться от одного корпоративного маршрутизатора в магистраль провайдера, затем поступать на корпоративный магистральный (центральный) маршрутизатор, затем передаваться обратно в провайдерскую магистраль и лишь затем поступать на оконечный (удаленный) маршрутизатор в пункте назначения. Поскольку удаленные маршрутизаторы подключаются к общей магистрали (магистрали сервис-провайдера), вариант, при котором трафик покидает магистраль, проходит через второй маршрутизатор и снова попадает в магистраль, нельзя признать эффективным.

Если сеть имеет полносвязную структуру (fully meshed), вышеуказанная ситуация не встречается, однако возникают другие проблемы. Корпорация должна платить за виртуальные каналы (а провайдер должен подкреплять их соответствующими сетевыми ресурсами), но при увеличении количества корпоративных отделений количество каналов

возрастает в геометрической прогрессии. Помимо высокой стоимости проблема усугубляется тем, что алгоритмы IP-маршрутизации плохо масштабируются в случае наращивания количества прямых связей между маршрутизаторами.

Одноранговая модель (Peer Model)

Для того, чтобы пользоваться услугами VPN, предприятию совсем не нужно проектировать и эксплуатировать собственную магистральную сеть. Сервис-провайдер, который уже имеет магистральную сетевую инфраструктуру, вполне может взять эту задачу на себя. Одноранговая модель VPN требует только подключения маршрутизатора заказчика к одному из маршрутизаторов сервис-провайдера.

В одноранговой VPN два маршрутизатора C считаются одноранговыми только в том случае, когда они находятся на одном сайте. Поэтому принадлежащий заказчику маршрутизатор C1 не имеет одноранговых (соседских) отношений с маршрутизатором C2, который принадлежит тому же заказчику, но установлен на другом сайте (в другом месте). Получается, что на каждом сайте заказчика имеется по крайней мере один корпоративный маршрутизатор (CE), связанный одноранговыми отношениями по крайней мере с одним маршрутизатором сервис-провайдера (PE).

CE-маршрутизаторы не обмениваются друг с другом данными о маршрутах. Нет вообще никакой необходимости в обмене какими-либо данными между CE-маршрути-заторами. Данные передаются от входящего CE-маршру-тизатора через входящий PE-маршрутизатор сервис-провайдера и проходят через один или несколько магистральных P-маршрутизаторов. В итоге они достигают исходящего PE-маршрутизатора сервис-провайдера и попадают на исходящий корпоративный CE-маршрутизатор. Таким образом маршрутизация становится оптимальной.

Поскольку CE-маршрутизаторы не обмениваются друг с другом

данными о маршрутах, корпорации не нужно иметь свою магистраль или управлять ею. Разумеется, корпоративный заказчик может пользоваться IP-магистралью так, как будто у него имеется сеть Frame Relay, и создавать своего рода «виртуальные каналы» между CE-маршрутизаторами. Обычно для этого используется одна из форм IP-туннелирования. Однако это приводит нас обратно к оверлейной модели со всеми ее проблемами. Одноранговая модель таких проблем не имеет.

Преимущества одноранговой модели

Одноранговая модель имеет целый ряд преимуществ:

1) В одноранговой модели количество работы, которую должен выполнить сервис-провайдер для технического обеспечения и управления VPN, прямо пропорционально количеству сайтов заказчика, подключенных к VPN. В оверлейной модели количество этой работы пропорционально квадрату сайтов заказчика, подключенных к VPN.

2) Одноранговая модель поддерживает оптимальную маршрутизацию пользовательского трафика по магистрали сервис-провайдера, так как в этой модели нет необходимости в транзитных CE-устройствах. Корпоративному заказчику не нужно управлять собственной магистралью. Ему нужно только подключить CE-маршрутизатор на каждом сайте.

Таким образом, одноранговая модель выгодна и сервис-провайдеру, и заказчику. Для провайдера она означает сокращение объема работ, а для корпоративного заказчика – более ценные услуги.

Трудности реализации одноранговой модели

Хотя одноранговая модель имеет множество преимуществ по сравнению с оверлейной, на пути ее реализации также стоит ряд проблем, которые перечислены ниже:

1) Перегрузка P-маршрутизаторов информацией о маршрутах. Одной из основных проблем крупных IP-магистралей является большое количество ресурсов (памяти, процессорных мощностей, полосы пропускания),

необходимых для хранения данных о маршрутизации. Если взять IP-магистраль и пустить по ней данные о маршрутах всех корпоративных сетей, P-маршрутизаторы никогда с ней не справятся.

2) Несогласованные (несмежные) адресные пространства. Обычно Интернет-сервис-провайдеры (ISP) стараются присваивать адреса осмысленно. Это значит, что адрес системы должен указывать на место, в котором эта система подключается к сети ISP. Однако многие корпоративные сети имеют адресные схемы, которые трудно совместить с магистральной топологией любого сервис-провайдера. В этих схемах адреса сайтов распределяются без какого-либо учета точки, в которой осуществляется подключение к провайдерской сети. Это сокращает возможности агрегации маршрутов и увеличивает объем данных о маршрутах, которые передаются по P-сети.

3) Частная адресация в C-сетях. Адреса во многих корпоративных сетях не являются уникальными. Это значит, что тот или иной адрес является уникальным только в пределах одного предприятия, но теряет уникальность при связи между предприятиями. Если IP-магистраль сервис-провайдера используется как общая магистраль для двух разных корпоративных сетей и если адреса в этих сетях не являются уникальными, P-маршрутизаторы не смогут гарантировать доставку пакетов по месту назначения.

4) Подслушивание. Для защиты данных нужно устанавливать шифрованные туннели «точка-точка» между каждой парой CE-маршрутизаторов (модель IPSec). Это решение хорошо подходит для оверлейной модели, полькольку она и без того использует туннель «точка—точка» между парами «соседних» CE-маршрутизаторов. Для одноранговой модели это решение подходит не столь хорошо, потому что здесь CE-маршрутизатор никогда не может определить, куда он будет передавать следующий пакет.

Варианты построения VPN

Можно выделить четыре основных варианта построения сети VPN, которые используются во всем мире. Вариант «Intranet VPN», который позволяет объединить в единую защищенную сеть несколько распределенных филиалов одной организации, взаимодействующих по открытым каналам связи. Именно этот вариант получил широкое распространение во всем мире, и именно его в первую очередь реализуют компании-разработчики.

Вариант «Remote Access VPN», который позволяет реализовать защищенное взаимодействие между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который подключается к корпоративным ресурсам из дома (домашний пользователь) или через notebook (мобильный пользователь). Данный вариант отличается от первого тем, что удаленный пользователь, как правило, не имеет статического адреса, и он подключается к защищаемому ресурсу не через выделенное устройство VPN, а прямиком со своего собственного компьютера, на котором и устанавливается программное обеспечение, реализующее функции VPN. Компонент VPN для удаленного пользователя может быть выполнен как в программном, так и в программно-аппаратном виде. В первом случае программное обеспечение может быть, как встроенным в операционную систему, так и разработанным специально. Во втором случае для реализации VPN используются небольшие устройства класса SOHO (Small OfficeHome Office), которые не требуют серьезной настройки и могут быть использованы даже неквалифицированным персоналом.

Вариант «Client/Server VPN», который обеспечивает защиту передаваемых данных между двумя узлами (не сетями) корпоративной сети. Особенность данного варианта в том, что VPN строится между узлами, находящимися, как правило, в одном сегменте сети, например, между

рабочей станцией и сервером. Такая необходимость очень часто возникает в тех случаях, когда в одной физической сети необходимо создать несколько логических сетей. Например, когда надо разделить трафик между финансовым департаментом и отделом кадров, обращающихся к серверам, находящимся в одном физическом сегменте.

В проекте принято решение использовать VPN-решения на базе сети провайдера Ангола-Телеком, по схеме «Intranet VPN».

[5,6,7]

3 РАЗРАБОТКА МУЛЬТИСЕРВИСНОЙ СЕТИ СВЯЗИ В ЦЕНТРАЛЬНОМ ОФИСЕ Г.ЛУАНДА

3.1 Выбор оборудования IP-АТС

Для организации сети Центрального офиса в г.Луанда принято решение заменить существующую учрежденческую АТС на современное оборудование – IP-АТС, которая называется PBX.

На рынке телекоммуникационного оборудования большое количество предложений, но при выборе учтены ряд условий:

- требуемые виды услуг (телефония, доступ в Интернет, ТВ, видеонаблюдение, видеоконференцсвязь);

- оборудование должно иметь сертификат и разрешение на использование в корпоративных сетях Республики Ангола;

- оборудование должно обеспечивать возможность выхода на внешние сети передачи данных и сети связи общего пользования;

- оборудование должно быть надёжным, и иметь приемлемую стоимость.

Рассмотрим основные характеристики IP-АТС разных производителей, чтобы сравнить их возможности и сделать выбор.

IP АТС

IP АТС – это многофункциональная телефонная система, коммутирующая голосовые и видео вызовы по IP сети. Голос и видео передаются как поток данных (IP пакеты). Наряду с перспективными технологиями коммуникаций, IP АТС предлагает отличное масштабирование ресурсов и повышенную надежность. Подключение к привычным аналоговым телефонным, цифровым или GSM линиям возможно с помощью опциональных недорогих VoIP шлюзов, поэтому переход от устаревшей АТС на современные корпоративные коммуникации

не вызовет особых сложностей. Компании даже не придется прерывать предоставление телефонных сервисов – IP АТС разворачивается параллельно с существующей станцией. В определенный момент, когда все будет подключено и протестировано, имеющиеся телефонные линии просто переключаются в новые IP шлюзы. Компания сохраняет свои старые, известные всем номера, а IP шлюзы преобразуют голос из других технологий в IP пакеты, с которыми работает IP АТС.

Принцип работы IP АТС

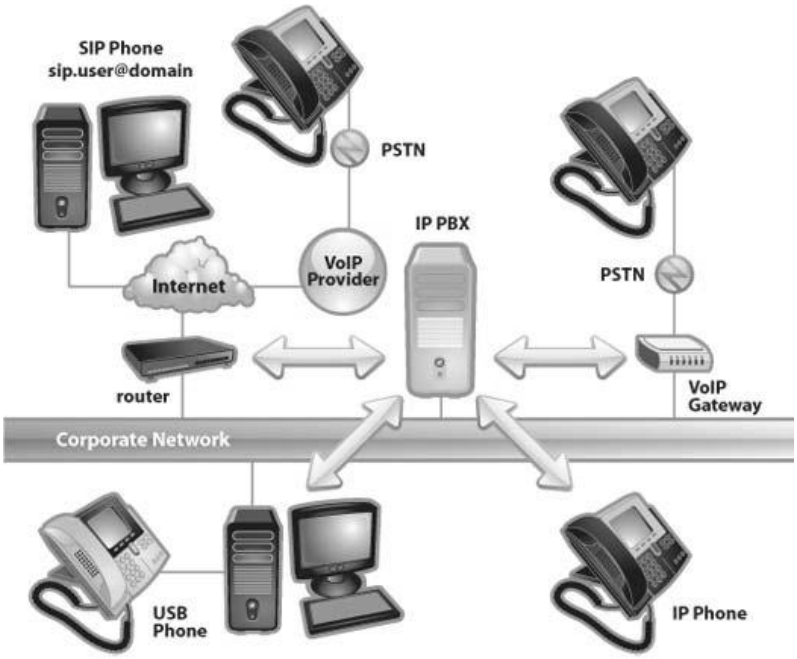

Рисунок 3.1 - Интеграция IP АТС в корпоративную сеть [10]

IP АТС, или корпоративная телефонная IP система, состоит из сервера IP АТС, нескольких SIP телефонов и, опционально, VoIP шлюзов для подключения к существующим телефонным сетям. Сервер IP АТС работает аналогично почтовому серверу – SIP клиенты (аппаратные и программные IP телефоны) регистрируются на сервере и уведомляют его, когда хотят выполнить вызов. IP АТС поддерживает каталог (базу данных) SIP адресов пользователей (добавочных номеров) и соответствующих им SIP устройств. По информации из каталога, IP АТС коммутирует пользователей внутри системы, маршрутизирует входящие вызовы на нужное SIP устройство и

маршрутизирует исходящие вызовы на соответствующий VoIP шлюз или VoIP провайдер.

IP АТС работает как сервис на компьютере с ОС Windows. Она использует расширяемые ресурсы серверной платформы и обладает простым интерфейсом, характерным для Windows приложений. Любой сотрудник, знакомый с Windows и основами сетей, может установить и поддерживать IP АТС. В то же время для внедрения традиционной АТС придется приглашать компанию-интегратора или проводить дорогостоящее сертифицированное обучение сотрудников.

IP АТС управляется через удобный и понятный пользователю графический интерфейс, доступный как через Windows консоль, так и через веб браузер. Традиционные аппаратные АТС зачастую имеют сложный системный интерфейс, разобраться с которым может только приглашенный сертифицированный наладчик.

IP АТС позволяет напрямую подключиться к ведущим VoIP операторам, предоставляющим международные вызовы по существенно сниженным ценам. И даже местные VoIP линии от телекоммуникационных компаний обойдутся вам существенно дешевле, чем аналогичные по емкости аналоговые или цифровые каналы. Если ваша компания имеет несколько филиалов, IP АТС в этих филиалах можно объединить между собой и звонить внутри компании совершенно бесплатно.

IP телефоны подключаются к сетевому коммутатору как обычные сетевые устройства. Затем они логически регистрируются на сервере IP АТС. Все современные IP телефоны имеют двухпортовый свитч и включаются “в разрыв” между сетевой розеткой и LAN портом компьютера. Кроме того, многие IP телефоны получают электропитание по технологии PoE. Программные IP телефоны можно установить на компьютер или смартфон. То есть, не нужно устанавливать и обслуживать дополнительную телефонную кабельную разводку. Благодаря поддержке PoE не потребуются

и дополнительные электрические розетки, т.к. телефоны получают электропитание по LAN кабелю. Также можно легко перемещать телефоны сотрудников, поскольку добавочный номер теперь не привязан к физической розетке.

IP АТС использует стандартный и открытый SIP протокол. Это значит, что к ней можно подключить любое стандартное SIP оборудование – IP телефоны и VoIP шлюзы любого производителя. Кроме того, к ней можно подключить IP линии от наиболее выгодного для вас VoIP оператора. Традиционные или проприетарные АТС, как правило, позволяют подключить только их собственные (весьма недешевые) IP телефоны и работают только с определенными, сертифицированными производителем, VoIP операторами. Различные дополнительные опции, такие как голосовая почта, также требуют приобретения специфических плат расширения данного производителя, которых часто не оказывается в наличии.

IP АТС работает на компьютере и ее расширяемость ограничивается только мощностью данного компьютера и пропускной способностью сети. На нынешнем этапе развития серверов IP АТС может обслуживать десятки тысяч пользователей, просто добавляя IP телефоны.

Благодаря интеграции IP АТС с популярными пользовательскими приложениями, как правило, CRM системами, можно повысить уровень обслуживания клиентов. При входящем вызове CRM система откроет “карточку” клиента со всеми прошлыми сделками, предпочтениями и прочей информацией.

Сотрудник будет готов к разговору заранее. Когда же сотруднику нужно перезвонить клиенту, или обзвонить группу клиентов, чтобы сообщить о новом предложении, он сделает это нажав кнопку Вызов из карточки, или запустив процесс автоматического обзвона отобранной группы. В обоих случаях это принципиально повышает производительность

персонала, позволяя обслужить больше клиентов меньшим количеством сотрудников.

Преимущество программной IP АТС заключается в том, что разработчики могут оперативно и недорого добавлять новые функции, и устранять проблемы в имеющихся. Все современные IP АТС уже включают опции, ранее доступные только в дорогих системах высшего класса – интерактивное голосовое меню, систему голосовой почты, группы и очереди дозвона, встроенную систему отчетов, интеграцию с CRM и многое другое.

Современный бизнес не привязан к одному месту. Сейчас вошло в норму частое перемещение сотрудников между рабочими местами, филиалами, странами. IP АТС идеально подходит для таких мобильных сотрудников, поскольку не требует перекоммутации или подвода телефонных линий.

Если пользователю нужно поработать в другом месте, он просто забирает свой настольный IP телефон с собой и включает в сеть в новом месте. В командировке достаточно запустить программный SIP телефон на ноутбуке или смартфоне, и сотрудник уже на связи. Благодаря возможностям протокола SIP, вызовы автоматически направляются в то место и на то устройство, откуда в данный момент подключен пользователь.

IP АТС имеет клиентское приложение под Windows с интуитивно понятным интерфейсом, в котором любая сложная операция выполняется несколькими кликами мыши. В этом же приложении сотрудник видит статусы своих коллег, активные вызовы в системе, состояние очередей вызовов и другую оперативную информацию. Некоторые из этих функций доступны и в традиционных АТС, однако требуют приобретения дорогих системных консолей или дополнительного платного программного обеспечения. Зачастую для “расшифровки”, отображаемой на системной консоли информации требуется специальная подготовка. [10]

3.2 Обзор оборудования IP PBX различных производителей

Внедрение IP АТС сейчас оправдано не только в новых компаниях, но и в существующих, поскольку предоставляет неоспоримые преимущества – резкое сокращение затрат на обслуживание и расширение, гибкую настройку, экономию на вызовах, повышение мобильности и производительности сотрудников. Если компания стремится быть лидером рынка, IP АТС является оптимальным решением. Для выбора оборудования для сети ГК Odebrecht рассмотрены и сравнены технические характеристики и особенности реализации IP PBX различных производителей.

IP-АТС Panasonic [13]

Компания Panasonic предлагает на рынке две IP-платформы (IP-АТС): KX-NS1000 и KX-NS500.

Рисунок 3.2 - IP-АТС Panasonic серии KX-NS

KX-NS1000 IP-АТС Panasonic

IP-платформа KX-NS1000 – наиболее мощный продукт компании. Она снимает ограничения по количеству внешних IP-транков и числу внутренних абонентских линий, свойственные предыдущим моделям АТС Panasonic. Поэтому она хорошо подходит для модернизации и развития корпоративной сети связи компаний любого масштаба.

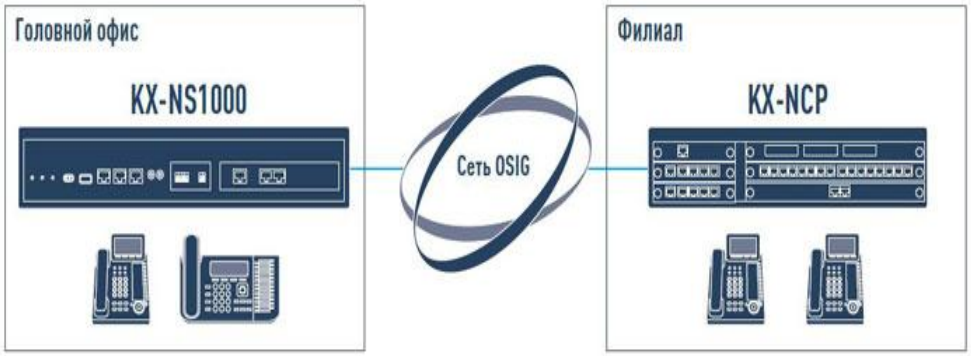

Рисунок 3.3 - IP-платформа KX-NS1000

Платформа KX-NS1000 может быть подключена к уже установленным в офисе АТС Panasonic серий KX-TDE и KX-NCP.

Вместе с тем KX-NS1000 – это именно IP-АТС, обладающая богатым функционалом за счет интеграции аппаратного и программного обеспечения. Ее применение наиболее целесообразно в компаниях, планирующих максимально использовать возможности IP-телефонии и современной системы телефонной связи в целях повышения эффективности бизнес-коммуникаций.

Единая сеть на базе KX-NS1000 с возможностью централизованного управления позволяет обеспечить надежную коммуникацию компании с филиалами, складами, а также удаленными сотрудниками, находящимися вне офисов. При этом IP-телефония позволяет оптимизировать расходы компании на связь. Переход на IP-телефонию позволяет таким компаниям экономить в среднем от 30 до 90% расходов на связь благодаря демократичным ценам провайдеров IP-телефонии.

Кроме экономии на внешних коммуникациях, KX-NS1000 позволяет организовать удобную и фактически бесплатную внутреннюю связь по IP-сети между отдельными офисами. Плата за все внутренние звонки будет минимальной, поскольку входит в стоимость интернет-трафика.

Но эффект от внедрения IP-платформы KX-NS1000 не ограничивается только экономией расходов на связь. Повышение качества работы персонала

вследствие перехода на коммуникации по новому стандарту – еще один фактор, способствующий увеличению прибыли компании. Встроенная голосовая почта, факс-сервер, колл-центр, интеграция телефонии с CRM-системой – все это позволяет выбрать оптимальный по цене и качеству способ общения с коллегами и заказчиками и сократить время выполнения рутинных операций. Ни один входящий звонок не останется без ответа, поскольку будет быстро перенаправлен по адресу даже в случае отсутствия сотрудника на рабочем месте.

Функциональные возможности IP-АТС KX-NS1000

IP-платформа Panasonic KX-NS1000 поддерживает все функции, которыми пользуются абоненты АТС предыдущих линеек KX-TDA/TDE/NCP компании Panasonic, а также предлагает новые, актуальные в современной бизнес-среде. Для доступа к некоторым функциям требуются ключи активации, другая часть функций доступна по умолчанию. Отдельные функции ранее были реализованы в качестве опций в виде внешних блоков, подключаемых к УАТС, а сейчас вошли в состав базовой комплектации станции.

Организация сетевой АТС с централизованным управлением

Сетевая IP-платформа. До 16-ти территориально удаленных блоков KX-NS1000 можно объединить в одну сеть. В такой сети все блоки работают как единая АТС. Все внутристанционные функции прозрачны. Контроль, программирование и управление сетью может выполняться из одной точки. Если перед компанией стоит задача организовать связь с территориально распределенными офисами, то сеть на базе IP-АТС Panasonic KX-NS1000 – хороший выбор.

Масштабируемость. Для компаний любого масштаба очень важно предусмотреть возможность расширения емкости системы в дальнейшем при минимальных вложениях. Функционал станции в дальнейшем может быть расширен с помощью ключей активации, а при необходимости к ней

можно подключить и модели предыдущей линейки АТС Panasonic, что позволит использовать и традиционную телефонию.

Отказоустойчивость. Компании любого сегмента рынка, особенно крупного бизнеса, уделяют особое внимание надежности оборудования. Сетевая АТС на базе IP-платформы KX-NS1000 обладает высокой отказоустойчивостью за счет резервирования элементов системы. При временном разрыве соединения сетевая система будет работать и сотрудники компании всегда будут оставаться на связи.

Единый внутренний номер. Новая IP-платформа позволяет присваивать каждому сотруднику компании короткий единый внутренний номер, к которому будут подключены до трех телефонов, включая традиционный, мобильный и SIP-телефон. Для связи с абонентом достаточно набрать его короткий внутренний номер, и он ответит по одному из этих телефонов в зависимости от того, где находится в данный момент.

Panasonic KX-NS500 — IP-АТС для малых и средних предприятий

Communication Assistant (CA). Это клиент-серверное приложение компьютерной телефонии обеспечивает управление телефоном с компьютера. Его серверная часть уже встроена в IP-платформу KX-NS1000, и для того чтобы воспользоваться возможностями приложения, нужно лишь установить клиентскую часть на компьютеры сотрудников офиса. Приложение включает большую записную книжку с возможностью разбиения абонентов по группам. Можно совершить вызов абонента в один клик, переадресовать вызов или поставить на удержание, собрать конференцию — все это делается просто, быстро и удобно. Всплывающее окно с информацией о звонящем клиенте, возможность интеграции с CRM-системой – это еще не полный перечень возможностей приложения Communication Assistant. Для менеджеров по продажам приложение CA — незаменимый инструмент в работе. Доступна также мобильная версия приложения.

Автосекретарь DISA. Автосекретарь – стандартная функция для всего модельного ряда АТС Panasonic. Голосовое приветствие, многоуровневое меню, возможность донабора внутреннего номера абонента – все это стандартные и привычные функции. В IP-АТС KX-NS1000 по умолчанию доступны 64 канала DISA.

Расширенные функции голосовой почты. Кроме DISA в АТС можно использовать автосекретарь UM (Unified Messaging), поскольку IP-платформа KX-NS1000 имеет встроенный речевой процессор или, правильнее сказать, единую систему обмена сообщениями UM. В предыдущих сериях АТС Panasonic требовалось приобрести отдельный блок речевого процессора, теперь же такая необходимость отпала. Как следствие, можно легко создавать корпоративные и индивидуальные голосовые почтовые ящики (1024 почтовых ящика для каждого блока NS1000).

IP-АТС KX-NS500 позволяет обеспечить IP-связью сотрудников, работающих в удаленном режиме, а также мобильных пользователей.

Запись телефонных разговоров. Такая функция востребована многими заказчиками. Контроль качества обслуживания клиентов, разрешение спорных ситуаций, выявление нелояльных сотрудников – все эти задачи решаются с помощью записи разговоров.

Контакт-центр. В IP-платформе KX-NS1000 встроена функция маршрутизации вызовов для организации контакт-центра без внешнего CTI-сервера. На базе этой функции можно создавать и более сложные решения для клиентских центров, в которых могут применяться голосовая почта, приложение Communication Assistant и CTI-приложения сторонних производителей.

Факс-сервер. Факс-сервер системы KX-NS1000 способен принимать, распределять и отправлять факсимильные сообщения. Принятый факс можно сохранить в почтовом ящике (об этого пользователя информирует

индикатор ожидающего сообщения), а также перенаправить, распечатать или загрузить.

Маршрутизация и VPN. Для достижения необходимого уровня безопасности коммуникаций применяют технологии виртуальных частных сетей (VPN) на участках АТС – АТС, АТС – IP-телефон и IP-телефон – IP-телефон. Платформа может работать в качестве маршрутизатора, а также имеет возможность настроить до 32 безопасных VPN-туннелей для каждого блока KX-NS1000.

IP-АТС CISCO [26]

Cisco Unified Communications Manager Express (CME, CUCME) – телефонная станция на базе роутеров моделей Cisco ISR 28xx (EoS), 29xx, 38xx (EoS), 39xx, которая не обеспечивает отказоустойчивость и позволяет построить телефонию до 100-150 абонентов, имеет возможность установить аналоговые и цифровые интерфейсы. Модель Cisco 2821 представляет собой производительный маршрутизатор, оснащенный двумя портами стандарта Gigabit Ethernet. Cisco 2821 имеет большие возможности конфигурации и расширения.

Cisco Business Edition 6000 (BE6k) – программно-аппаратный комплекс на базе сервера Cisco UCS C220 M3, поддерживающий отказоустойчивость, емкость до 1000 пользователей. В состав BE6k входит АТС – Cisco UCM, сервер голосовой почты – Cisco Unity Connection (CUC), сервер состояний присутствия и Jabber клиента – Instant Messaging and Presence (IM&P), контакт-центр до 100 операторов – Cisco Unified Contact Center Express (UCCX) и многое другое.

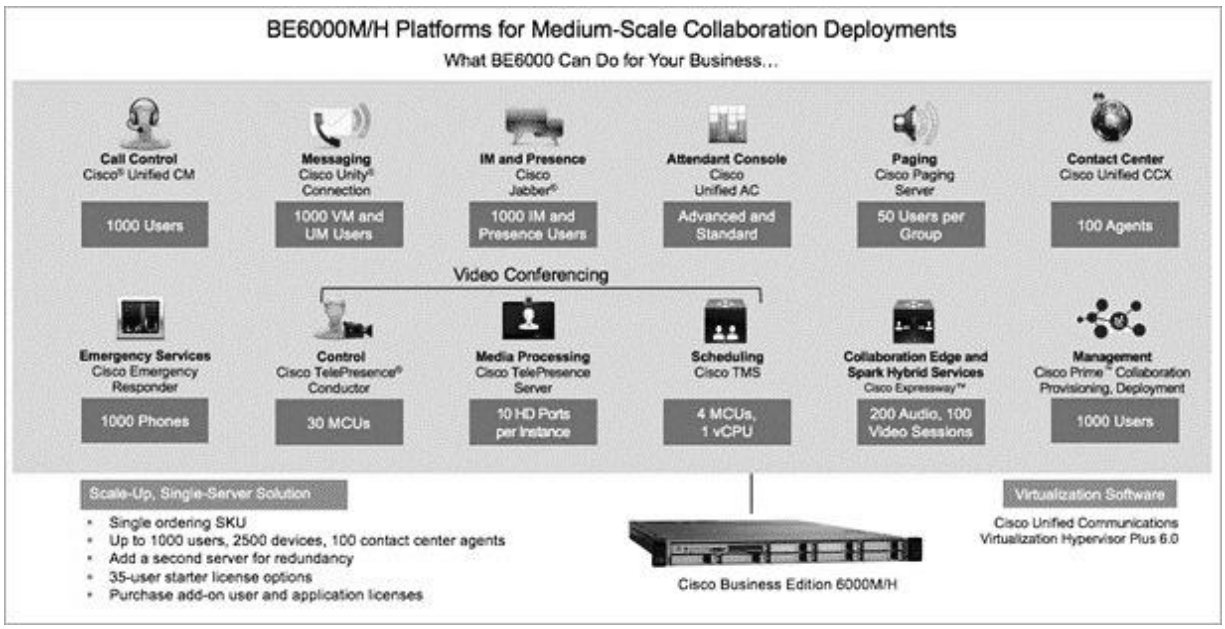

Рисунок 3.4 – Характеристики платформы Cisco Business Edition 6000

Коммуникационный центр для совместной работы, унифицированных и видеокоммуникаций, а также контактный центр на базе решения Cisco Business Edition 6000 ориентирован для работы в компаниях среднего бизнеса с численностью абонентов от 200 до 1000 сотрудников, работающих не более чем в 50 офисах.

Данное решение размещается на одном сервере (два - для отказоустойчивости, кластер) и обеспечивает функционирование следующих сервисов:

• Высококачественную голосовую связь по всей компании: в офисах, на производственных площадках, складах и в каждом месте нахождения сотрудника

• Короткий набор номера, единый справочник абонентов, управление доступом к телефонной сети и множество других функций корпоративной телефонии

• Использование мобильных устройств пользователей (мобильные и планшетные компьютеры, коммуникаторы) в качестве «телефонов» для безопасной мультимедийной связи с коллегами (семейство программных

клиентов Cisco Jabber для Windows, Mac, iOS, Android и других устройств) независимо от того, где сотрудники находятся

• HD-видеокоммуникации и взаимодействие с системами Cisco TelePresence

• Сервисы мгновенного обмена текстовыми сообщениями (IM)

• Сервисы контроля доступности абонентов (Presence), интегрированных с корпоративным календарем

• Полнофункциональный контактный центр (100 рабочих мест операторов), обслуживающий голосовые, видео- и Интернет-обращения

• Унифицированная голосовая почта

• Простая система управления и администрирования, понятная для специалистов систем связи и телефонии

• Встроенная система статистики звонков, мониторинга состояния компонентов системы и поиска неисправностей

Cisco Business Edition 6000 активно использует технологии виртуализации и автоматизации типовых операций администрирования, поддерживает дружественный интерфейс пользователя (на русском языке) и многолетний опыт компании Cisco в области построения отказоустойчивых систем связи в распределенной среде, что позволяет предприятиям среднего бизнеса заметно сократить стоимость владения системой за счет сокращения времени, необходимого для ее обслуживания и времени простоев, связанных с ошибками эксплуатации.

Коммуникационный центр на базе Cisco Business Edition 6000 включает в себя сервер Cisco Unified Computing System™ (UCS) (стоечный сервер высокой плотности), на котором разворачиваются следующие сервисы:

• Cisco Unified Communications Manager (IP-АТС)

• Cisco Unity® Connection (унифицированная голосовая почта)

• Cisco Unified Presence (контроль доступности абонента и мгновенный обмен сообщениями)

• Cisco Unified Contact Center Express (контактный центр для обслуживания голосовых и видеообращений, и обращений из сети Интернет – email, web-формы и так далее)

• Cisco Unified Provisioning Manager (автоматизация процесса администрирования всех приложений системы в рамках простого веб-интерфейса пользователя).

Цена – 6580 $ [25]

IP АТС LG-Ericsson iPECS LIK [27]

Рисунок 3.5 - IP АТС LG-Ericsson iPECS LIK

iPECS LIK - это принципиально новая IP АТС от компании LG-Ericsson, основной особенностью которой является полностью распределенная, модульная IP архитектура. Такая архитектура позволяет легко объединять территориально удаленные объекты в единую систему для передачи голоса, видео и данных. Система может обладать большим количеством узлов, к которым при необходимости очень просто добавить новые. Еще одним существенным достоинством iPECS-IK является привлекательная цена.

IP телефония

Основной особенностью и преимуществом iPECS LIK является ее архитектура. Ядром системы является центральный модуль (процессор), который обеспечивает взаимодействие между остальными модулями и

терминалами системы на основе собственного iPECS протокола, распределяет системные ресурсы и обеспечивает процесс коммутации.

К этому процессору подключаются все остальные модули системы. Причем расположены эти модули могут быть где угодно, т.к. подключение осуществляется либо по локальной сети, либо через Интернет.

Таким образом, чтобы подключить удаленный офис или другой удаленный объект (склад, магазин, домашний офис и т.п.) достаточно в нем установить соответствующие модули и настроить соединение с центральным процессором. При росте количества абонентов или удаленных офисов просто подключаются дополнительные модули.

Такая архитектура накладывает и определенные требования на пропускную способность канала, к которому подключен центральный процессор, т.к. процессор должен пропускать "через себя" трафик абонентов, в т.ч. и удаленных. Но здесь есть ряд факторов, которые позволяют компенсировать данную нагрузку:

- Сетевая инфраструктура постоянно развивается, и получить канал нужной пропускной способности становится проще и дешевле.
- Как правило абоненты не разговаривают все одновременно, поэтому при расчете пропускной способности можно принять соотношение одновременных разговоров к общему числу абонентов как 1:3
- Голосовой трафик между IP абонентами или абонентами одного локального узла проходит не через процессор, а напрямую между абонентами.

Функции IP телефонии

1. Просто организовать корпоративную сеть из 2-х и более АТС, объединенных по IP-каналам.

Это позволит существенно экономить на переговорах между различными подразделениями компании, эффективно организовать рабочий процесс внутри компании, централизованно использовать ресурсы АТС.

Кроме того, iPECS LIK LG может быть легко интегрирована в сеть с другими системам производства LG-Ericsson - ipLDK и iPECS-MG

2. Просто организовать удаленный филиал или рабочее место на дому.

Использование IP телефонов или IP софтфонов позволит обеспечить сотрудников полным доступом к функциям головной АТС, так, как если бы они находились в офисе, тем самым оптимизировав затраты на построение сети

3. Подключение внешних IP линий.

Многие операторы связи предлагают подключить внешние линии по IP каналам, что как павило существенно проще и дешевле традиционного подключения. Также упрощается организация многоканального номера или, например, подключение прямого номера какого-нибудь крупного города, в котором у Вас есть клиенты или партнеры

4. Безопасность и качество обслуживания (QoS).

IP АТС iPECS-LIK поддерживает несколько протоколов безопасности и приоритетов для обеспечения необходимого уровня безопасности и качества голоса в сетевой среде. IPsec, sRTP, TLS - хорошо известные стандарты безопасности, с помощью которых выполняется кодирование данных в IP пакетах. Для скрытия истинного адреса назначения пакета используется современная техника кодирования и тунелинга. Для обеспечения наивысшего показателя качества речи iPECS-LIK поддерживает стандарты DiffServ pre-tagging и 802.1 p/Q WALN технологию. Также для улучшения качества передачи голоса IP АТС использует функцию эхоподавления.

5. IP телефоны позволяют создать удаленные рабочие места

Это позволяет снизить затраты на организацию удаленных рабочих мест или филиалов за счет использования выделенных IP каналов или Интернета

6. Использование в качестве инфраструктуры только одной сети – компьютерной.

Используя на рабочих местах только IP телефоны, Вам не понадобится создавать 2 различных сети – компьютерную и телефонную, что позволит существенно сэкономить на материалах и работах по прокладке телефонной сети, а также по ее обслуживанию. Системные IP телефоны LG-Ericsson серии LIP-8000 имеют 2 Ethernet порта, один из которых подключается в LAN сеть, а в другой подключается ПК абонента.

Сетевые возможности

Возможность организации единой корпоративной сети связи.

Единая нумерация - звонки между разными офисами компаний простым набором внутреннего номера, даже если офисы находятся в разных странах Удобство в работе - можно переключать звонки на сотрудника любого офиса, выходить на внешние линии другого офиса, создавать территориально распределенные Call-центры, службы техподдержки и т.д. Плюс существенная экономия на междугородних и международных переговорах за счет аренды выделенных линий связи или интернет-каналов. Все модули системы iPECS-LIK взаимодействуют между собой по IP-протоколу и включаются в сеть Ethernet, что позволяет им работать как в локальной сети, так и в глобальной. Возможна работа модулей из-под NAT, но лучше строить VPN или дать каждому удаленному модулю внешний ip-адрес. В принципе известны порты работы IPKTS протокола, поэтому можно организовать DMZ. Работа в одной сети позволяет после соединения абонентов отправлять голосовой поток непосредственно с модуля на модуль, что улучшает и качество, и устойчивость соединения, а в случае, когда они оба находятся под разными NAT, голосовой поток вынужденно будет коммутироваться процессором управления.

Ёмкость

Емкость iPECS-LIK определяется процессором. Существуют следующие типы процессоров:

- LIK-50: емкость до 50 портов.
- LIK-100: емкость до 100 портов.
- LIK-300: емкость до 300 портов
- LIK-600: емкость до 600 портов
- LIK-1200: емкость до 1200 портов

Система обладает распределенной модульной архитектурой с возможностью расширения.

Мобильность

Микросотовая сеть предоставляет возможность перемещаться по территории офиса, предприятия или коттеджа с радиотелефоном стандарта DECT, оставаясь при этом всегда на связи. Особенно важна такая связь для сотрудников, которые не сидят на одном месте, а часто перемещаются по территории. Застать его на рабочем месте сложно, а так он всегда будет на связи, а также микросотовая сеть дает возможность обеспечить связь там, куда сложно или невозможно протянуть провода для установки стационарных телефонов

iPECS-LIK50/100 обеспечивают подключение до 16-и модулей базовых станций WTIM.

iPECS-LIK300/600 обеспечивают подключение до 32-х модулей базовых станций WTIM.

Для сети из нескольких АТС доступна функция DECT роуминга, т.е. абонент с DECT трубкой может перемещаться в пределах сети, при этом его трубка будет регистрироваться в сети DECT локального офиса с сохранением своего внутреннего номера.

Сеть Wi-Fi

Использование для передачи голоса беспроводной сети передачи данных Wi-Fi. Используя сеть стандартных точек доступа Wi-Fi можно обеспечить полный доступ к ресурсам IP АТС iPECS LIK на всей территории покрытия сети. Для осуществления такого доступа используются беспроводные IP телефоны LG-Ericsson - современные Wi-Fi телефоны с применением шифрования и доступом в Интернет.

Резервирование системы

Помимо основного процессора в удаленных офисах можно устанавливать свои локальные процессоры, которые будут перехватывать управление, если будет потеряна связь с центральным процессором. Как только связь будет установлена, управление вновь перейдет к основному процессору. Таким образом, локальный процессор обеспечивает работоспособность локального офиса и, в зависимости от конфигурации, позволяет обеспечить сервис дублирующей поддержки сети общего пользования (для обеспечения отказоустойчивости) в отношении внутренних вызовов. . [8, 9, 10, 11]

3.3 Выбор IP-АТС

Сравнение основных технических характеристик станций, поддерживающих голосовые сервисы и работающих в сетях с пакетной коммутацией, показало, чтовсе они обладают достаточным потенциалом для исользования в проекте. При выбре компании-производителя учитывается также её имидж и надежность. Одним из лидеров на рынке комплексных решений является корпорация Cisco (США). Cisco поставляют заказчикам комплексные решения, включающие вычисление, сеть, средства хранения данных, безопасность и сервисы L4-7. Кроме того, они предоставляют

большое количество опций и много возможностей масштабирования центров обработки данных.

С учетом количества пользователей (сотрудников филиала), выбрана платформа Cisco Business Edition 6000.

Cisco Business Edition 6000 позволяет предприятиям среднего бизнеса эффективно использовать преимущества современных технологий коммуникаций для создания конкурентных преимуществ за счет:

• повышения эффективности совместной работы с коллегами, партнерами и клиентами,

• уменьшения сроков принятия решений,

• ускорения вывода на рынок новых продуктов,

• сокращения эксплуатационных расходов.

3.3.1 Выбор оборудования для организации сети офиса

В офисах компании планируется использовать архитектуру Ethernet, ядром которой будет выбранная IP-АТС, в состав которой входят: маршрутизирующий коммутатор уровня L3, шлюзы во внешние сети, proxy-серверы. Для реализации распределительной сети необходимо использовать коммутаторы уровня агрегации и доступа. Принято решение, для обеспечения легкости настройки и совместимости с АТС Cisco Business Edition 6000 всех сетевых компонентов, выбрать оборудование компании Cisco Inc. (США), включая: коммутаторы для создания подсети офиса, IP-телефоны пользователей, маршрутизаторы для организации виртуальной частной сети.

Коммутатор Cisco WS-C2960G-24 [18]

Интеллектуальные Ethernet-коммутаторы Cisco Catalyst серии 2960 (Cisco Catalyst 2960 Series Intelligent Ethernet Switch) позволяют реализовать расширенные сервисы в локальных сетях крупных и средних

предприятий, а также в сетях филиалов. Представители этого семейства автономных коммутаторов с фиксированной конфигурацией обеспечивают подключение рабочих мест на скоростях 10/100 Fast Ethernet и 10/100/1000 Gigabit Ethernet.

Рисунок 3.6 - Коммутатор Cisco WS-C2960G-24

Основные особенности:

- Высокий уровень безопасности, усовершенствованные списки контроля доступа (ACL);
- Организация контроля сети и оптимизация ширины канала с использованием QoS, дифференцированного ограничения скорости и ACL.
- Коммутаторы просты в управлении и конфигурирования
- Благодаря отсутствию вентилятора и бесшумной работе коммутатор органично вписывается в рабочую обстановку.
- USB-накопитель для резервного копирования, распространения данных и упрощения эксплуатации. . [12, 13, 14 , 16]

Межсетевой экран CISCO ASA5505-K8 ASA 5505 Appliance with SW [26]

Для обеспечения безопасного доступа к Интернет: Межсетевой экран CISCO ASA5505-K8 ASA 5505 Appliance with SW, 10 Users, 8 ports - ASA5505-K8 являются полнофункциональным комплексом безопасности для малого бизнеса, офисов и удаленно работающих сотрудников.

Оборудование имеет высокопроизводительный межсетевой экран, SSL и IPsec VPN, а также большое количество сетевых служб в модульном комплексе, поддерживающих "plug-and-play". Данная модель спользует

встроенный Cisco ASDM который быстро монтируется и настраивается. Имеет гибкий коммутатор на 8 портов, которые можно динамически сгруппировать для создания 3 отдельных виртуальных сетей, обеспечивая более высокую сетевую фрагментацию и защиту. ASA5505-K8 имеет 2 PoE (Power over Ethernet) порта, что способствует увеличению сетевой мобильности, облегчению установки IP-телефонии и беспроводных точек доступа. После добавления AIP SSC устройству становится доступно предотвращение вторжений и служба блокирования сетевых червей в системе. Небольшое количество портов USB можно использовать для увеличения дополнительных служб и возможностей.

Серверы

В качестве серверной платформы выбрано оборудование линейки Cisco Unified Computing System – серверная система для ЦОД нового поколения. Это единая система, включающая: вычислительные ресурсы; сетевую инфраструктуру уровня доступа; управление комплексом. Обеспечивает следующие функции: подключение серверов и виртуальных машин напрямую к центральному коммутатору; универсальный транспорт для передачи LAN, SAN и управления; гибкое распределение полосы пропускания, эффективное управление трафиком; интегрированное управление; возможность интеграции с партнерскими решениями.

Основные характеристики сервера Cisco UCSC-C240-M4S: UCS C240 M4 SFF, no CPU, memory, HDD, SSD, PCIe cards, tool-less rail kit, or power supply. [27]

Серверная платформа объединит, кроме стандарной поддержки сервисов стека протоколов TCP/IP, почтовых сервисов, DNS, DHCP, серверы аутентификации и авторизации AAA (Radius), систему учета расходования ресурса и тарификации Billing.

Проектируемая схема организации связи в Центральном офисе компании показана на рисунке 3.7

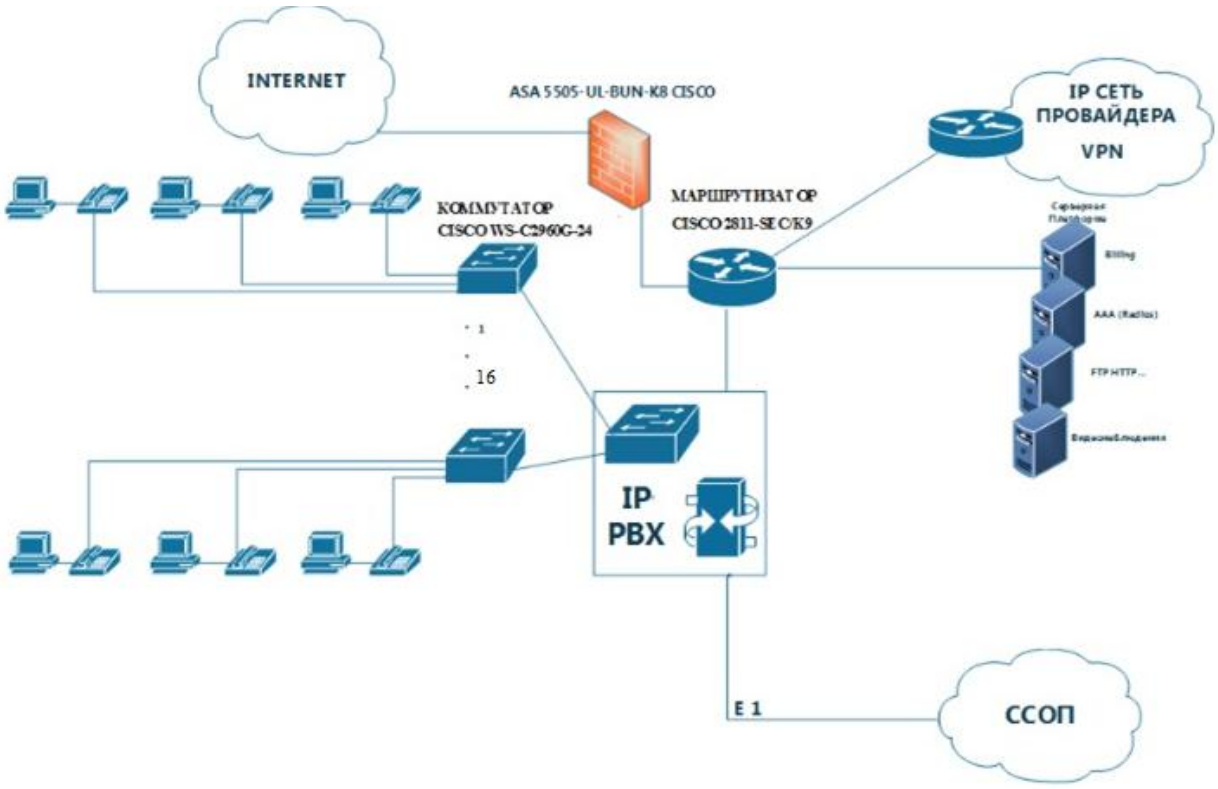

Рисунок 3.7 - Проектируемая схема организации связи в Центральном офисе г.Луанда

Для организации сети Центрального офиса в г.Луанда принято решение заменить существующую учрежденческую АТС на современное оборудование – IP-АТС фирмы Cisco Business Edition 6000.

3.4 Расчет нагрузок

Для расчета нагрузок взят филиал, находящийся в г. Луанда. В проектируемой сети связи основную полосу пропускания занимают услуги IP – телефонии, передачи данных внутри сети, и доступа к глобальной сети Internet (услуги Triply Play). Требуемая полоса пропускания для услуг Triply Play рассчитана с учетом необходимого запаса для предоставления оставшихся услуг.

Для правильной оценки характеристик и расчета требуемой пропускной способности для предоставления комплексной услуги Triply Play используем параметры, основанные на статистических данных. Проектируемая сеть должна быть надежной и на ней не должно быть перегрузок. Поэтому все необходимые расчеты трафика будем производить для часа наибольшей нагрузки для одного оптического сетевого узла.

3.4.1 Расчет трафика телефонии

Для организации услуг IP телефонии необходимо рассчитать требуемую полосу пропускания. Исходными данными для расчета являются:

- количество источников нагрузки – абоненты, использующие терминалы SIP и подключаемые в пакетную сеть посредством IP-АТС N_{SIP}=360 абонентов;

- тип кодека в планируемом к внедрению оборудовании, G.729A;

- длина заголовка IP пакета, 58 байт.

Транспортный ресурс, который должен быть выделен для передачи в пакетной сети телефонного трафика, поступающего на IP-АТС, при условии использования кодека определяется следующим образом:

Полезная нагрузка голосового пакета G.729A CODEC составит

$$У_{полезн} = \frac{t_{звуч.голоса} \cdot \upsilon_{кодирования}}{8 \, бит/байт} = ...байт, \quad (3.1)$$

где $t_{звыч.голоса}$ - время звучания голоса (мс), $\upsilon_{кодирования}$ - скорость кодирования речевого сигнала (Кбит/с).

Эти параметры являются характеристиками используемого кодека. В данном случае для кодека G.729A скорость кодирования – 8кбит/с, а время звучания голоса – 20 мс.

$$У_{полезн} = \frac{20 \cdot 8}{8} = 20 байт.$$

Каждый пакет имеет заголовок длиной в 58 байт.

Общий размер голосового пакета составит:

$$V_{\text{пакета}} = L_{Eth} + L_{IP} + L_{UDP} + L_{RPT} + Y_{полезн}, байт, \quad (3.2)$$

где $L_{\text{Eth, IP, UDP, RTP}}$ – длина заголовка Ethernet, IP, UDP, RTP протоколов соответственно (байт), $Y_{\text{полез}}$ – полезная нагрузка голосового пакета (байт).

$$V_{пакета} = 14 + 20 + 8 + 16 + 20 = 78 байт.$$

Использование кодека G.729A позволяет передавать через шлюз по 50 пакетов в секунду, исходя из этого, полоса пропускания для одного вызова определится по формуле:

$$ППр_1 = V_{паекта} \cdot 8^{бит}/_{байт} \cdot 50_{pps}, Кбит/с, \quad (3.3)$$

где $V_{\text{пакета}}$ – размер голосового пакета, [байт].

$$ППр_1 = 78 \cdot 8 \cdot 50 = 30 Кбит/с.$$

В проектируемой сети устанавливается IP-АТС, в которой задействовано 360 голосовых портов (офис Луанда). С помощью средств подавления пауз обычный голосовой вызов можно сжать примерно на 50 процентов (по самым консервативным оценкам – 30%). Исходя из этого, необходимая полоса пропускания WAN для работы IP-АТС составит:

$$ППр_{WAN} = ППр_1 \cdot N_{SIP} \cdot VAD, \text{Мбит/с}, \quad (3.4)$$

где $ППр_1$ – полоса пропускания для одного вызова, (Кбит/с), N_{SIP} – количество голосовых портов в точке присутствия, (шт), VAD (Voice Activity Detection) – коэффициент механизма идентификации пауз (0,7).

$$ППр_{WAN} = 30 \cdot 360 \cdot 0{,}7 = 7560\,кбит/с.$$

Результаты могли быть другими, если бы использовались другие средства кодирования/декодирования (CODEC), изменилась средняя продолжительность вызова. Кроме того, на конечный результат может повлиять тип используемого приложения. Так, например, передача музыки вызывающему абоненту, который ждет ответа оператора, не позволяет использовать средства подавления пауз.

3.4.2 Расчет трафика передачи данных

Сети передачи данных предназначены для совместного доступа пользователя к ресурсам компьютеров: приложениям, файлам, принтерам и т.п. а так же для передачи мультимедийного трафика. Трафик, создаваемый этими традиционными службами, имеет свои особенности и существенно отличается от трафика сообщений в телефонных сетях или сетях кабельного телевидения. Трафик компьютерных данных характеризуется крайне неравномерной интенсивностью поступления сообщений в сеть. Коэффициент пульсации трафика отдельного пользователя сети, равный отношению средней интенсивности обмена данными к максимально возможной, может достигать 1:50 и даже 1:100. Но если число абонентов, обслуживаемых коммутаторами, достаточно велико, то пульсации отдельных абонентов в соответствии с законом больших чисел

распределяются во времени так, что их пики не совпадают и коэффициент пульсации на магистральных каналах значительно снижается.

Среди всех пользователей сети в час наибольшей нагрузки (ЧНН) в сети будет находиться и передавать данные только часть абонентов (активные абоненты). Даже в час наибольшей нагрузки количество активных абонентов может изменяться, поэтому для их подсчета используется пятиминутный временной интервал внутри ЧНН, и максимальное число активных абонентов за этот период времени определяется параметром Data Average Activity Factor (DAAF), в соответствии с этим количество активных абонентов составит

$$AS = TS*DAAF, \text{ аб}, \quad (3.5)$$

где TS – число абонентов на одном сетевом узле для филиала в Луанде - 360, (аб), DAAF – процент абонентов, находящихся в сети в ЧНН.

$$AS = (360/21)*0,8= 14 \text{ абонентов}.$$

В час наибольшей нагрузки в сети находится 14 человек в офисе Луанда.

Абоненты время от времени передают и принимают данные и, как правило, объем передаваемых данных значительно меньше объема принимаемых данных. Каждому абоненту необходимо обеспечить заявленную пропускную способность. Далее определим среднюю пропускную способность сети, требуемой для обеспечения нормальной работы пользователей.

Средняя пропускная способность для приема данных составит:

$$BDDA = (AS*ADBS)*(1 + OHD), \text{ Мбит/с}, \quad (3.6)$$

где AS - количество активных абонентов, (аб), ADBS – средняя скорость приема данных, (Мбит/с), OHD – отношение длины заголовка IP пакета к его общей длине во входящем потоке.

$$BDDA = (14*2)*(1+0,1) = 30,8 \text{ Мбит/с}$$

Средняя пропускная способность для передачи данных

$$BUDA = (AS*AUBS)*(1 + OHU), \text{ Мбит/с}, \quad (3.7)$$

где AS - количество активных абонентов, (аб), AUBS – средняя скорость передачи данных, (Мбит/с), OHU – отношение длины заголовка IP пакета к его общей длине в исходящем потоке.

$$BUDA = (14*0,5)*(1+0,15) = 8,05 \text{ Мбит/с}$$

Количество абонентов, передающих или принимающих данные в течение некоторого короткого промежутка времени, определяют пиковую пропускную способность сети. Количество таких абонентов в час наибольшей нагрузки определяется коэффициентом Data Peak Activity Factor (DPAF)

$$PS = AS*DPAF, \text{ аб}, \quad (3.8)$$

где DPAF – процент абонентов, одновременно принимающих или передающих данные в течение короткого интервала времени.

$$PS = 14*0,7 = 10 \text{ абонентов}$$

Пиковая пропускная способность измеряется за короткий промежуток времени (1 секунда), она необходима для приема и передачи данных в

момент, когда одновременно несколько пользователей передают или принимают данные по сети. Пиковая пропускная способность, требуемая для приема данных в час наибольшей нагрузки:

$$BDDP = (PS*PDBS)*(1 + OHD), \text{ Мбит/с}, \quad (3.9)$$

где PDBS – пиковая скорость приема данных, Мбит/с.

$$BDDP = (10*3)*(1+0,1) = 30,3 \text{ Мбит/с}$$

Пиковая пропускная способность для передачи данных в ЧНН

$$BUDP = (PS*PUBS)*(1 + OHU), \text{ Мбит/с}, \quad (3.10)$$

где PUBS – пиковая скорость передачи данных, Мбит/с.

$$BUDP = (10*1,5)*(1+0,15) = 17,25 \text{ Мбит/с}$$

Из расчета видно, что пиковая пропускная способность для передачи данных выше средней пропускной способности.

Для проектирования сети необходимо использовать максимальное значение полосы пропускания среди пиковых и средних значений для исключения перегрузки сети:

$$BDD = Max [BDDA; BDDP], \text{ Мбит/с}, \quad (3.11)$$

$$BDU = Max [BUDA; BUDP], \text{ Мбит/с}, \quad (3.12)$$

где BDD – пропускная способность для приема данных, (Мбит/с), BDU – пропускная способность для передачи данных, [Мбит/с].

$$BDD = Max [30,8; 30,3] = 30,8 \text{ Мбит/с},$$

$$BDU = Max [8,05; 17,25] = 17,25 \text{ Мбит/с}$$

Общая пропускная способность для приема и передачи данных, необходимая для нормального функционирования оптического сетевого узла, составит

$$BD = BDD + BDU, \text{ Мбит/с}, \quad (3.13)$$

где BDD – максимальная пропускная способность для приема данных, (Мбит/с), BDU – максимальная пропускная способность для передачи данных, (Мбит/с).

$$BD = 30,8+17,25 = 48,05 \text{ Мбит/с}$$

Итак, для передачи данных между абонентами сети на одном сетевом узле офис Луанда необходима полоса пропускания 48,05 Мбит/с.

3.4.3 Расчет трафика предоставления услуг доступа к сети Internet

Все расчеты параметров проектируемой сети приводятся, принимая во внимание следующие исходные данные:

Только 10% из числа пользователей могут находиться в сети одновременно. Из них 20% в час наибольшей нагрузке (ЧНН). Из этих 20% только 25% загружают данные.

Определим число активных пользователей, работающих на средней скорости по формуле:

$$N_{act\ subser} = HHP * DP * DAAF, \text{ аб}, \quad (3.14)$$

где HHP – общее число абонентов проектируемой сети; DP – характеристика проникновения трафика данных; DAAF – фактор активности.

$$N_{act\ subser} = 360 * 0{,}1 * 0{,}2 = 8 \text{ абонентов.}$$

Далее рассчитаем количество абонентов одновременно принимающих и передающих данные по формуле:

$$Peak_{subser} = HHP * DP * DPeakAF, \text{ аб} \qquad (3.15)$$

$$Peak_{subser} = 360 * 0{,}1 * 0{,}1 = 4 \text{ абонентов}$$

Для определения требуемой полосы пропускания для среднего и пикового трафика необходимо рассчитать среднюю и пиковую полосу пропускания в ЧНН для восходящего и нисходящего трафика и выбрать из них максимальный.

$$BWDA = \left(N_{act\ subser} * BWA_{per\ subser}\right) * \left(1 + OH\right), \text{ Мбит/с,} \qquad (3.16)$$

$$BWDPeak = \left(Peak_{subser} * BWP_{per\ subser}\right) * \left(1 + OH\right), \text{ Мбит/с,} \qquad (3.17)$$

где $BWA_{per\ subser}$ - средняя полоса пропускания, приходящаяся на 1 абонента (1800 кбит/с); $BWP_{per\ subser}$ – пиковая полоса пропускания на 1 абонента (4000 кбит/с); ОН – отношение длины заголовка к длине пакета (0,1).

$$BWDA = \left(8 \cdot 1800\right) * \left(1 + 0{,}1\right) = 15840 \text{ кбит/с,}$$

$$BWDPeak = \left(4 * 4000\right) * \left(1 + 0{,}1\right) = 17600 \text{ кбит/с}$$

Для определения требуемой полосы пропускания определим максимальное значение между пиковой и средней пропускной способностью:

$$BWData = MAX\left[BWDA; BWDPeak\right], \text{ Мбит/с} \qquad (3.18)$$

$$BWData = MAX\left[15840; 17600\right] = 17600 \text{ кбит/с}$$

Таким образом, для реализации услуги доступа к глобальной сети Internet полоса пропускания каждого проектируемого узла должна составлять 17,6 Мбит/с.

Общая требуемая пропускная способность узла в Луанде составит:

$$ППр_{Triply\ play} = ППр_{WAN} + BD + BWData, \text{ Мбит/с,} \quad (3.19)$$

где $ППр_{WAN}$ – пропускная способность для трафика IP телефонии, (Мбит/с); AB – пропускная способность для видеопотоков, (Мбит/с); BD – пропускная способность для трафика данных, (Мбит/с); BWData - пропускная способность для предоставления услуги доступа к сети Internet, (Мбит/с).

$$ППр_{Triply\ play} = 7{,}56 + 48{,}05 + 17{,}6 = 73{,}21 \text{ Мбит/с}$$

Требования к пропускной способности узла сети в филиале Луанда будут удовлетворены при внедрении сетевых решений. [4].

Аналогично необходимо сделать расчеты в остальных офисах компании. Результаты расчетов сведены в таблицу 3.2.

Таблица 3.2 – Результаты расчета нагрузок

	ЛУАНДА	БЕНГЕЛА	ЗАИР	ЮЖНАЯ КВАНЗА	МАЛАНЖЕ	СЕВЕРНАЯ КВАНЗА
телефония	7,560 Мбит/с	6,552 Мбит/с	3,024 Мбит/с	3,528 Мбит/с	4,536 Мбит/с	5,544 Мбит/с
данные	48,05 Мбит/с	40,2 Мбит/с	20,1 Мбит/с	25,125 Мбит/с	30,15 Мбит/с	35,175 Мбит/с
Доступ в Интернет	17,6 Мбит/с	13,2 Мбит/с	8,8 Мбит/с	8,8 Мбит/с	13,2 Мбит/с	13,2 Мбит/с
ППр Triply play	73,21 Мбит/с	59,952 Мбит/с	31,924 Мбит/с	37,453 Мбит/с	43,486 Мбит/с	53,919 Мбит/с

Таким образом, оценив требуемую полосу пропускания, можно сделать расчет количества оборудования и создать схему организации связи.

3.5 Расчет объема оборудования

Расчет объема оборудования выполнен с учетом размещения оборудования на этажах и в серверной, количества портов коммутаторов, и назначения основных сетевых элементов.

Количество коммутаторов определено в зависимости от их расположения на этажах, как показано на рисунке 3.8.

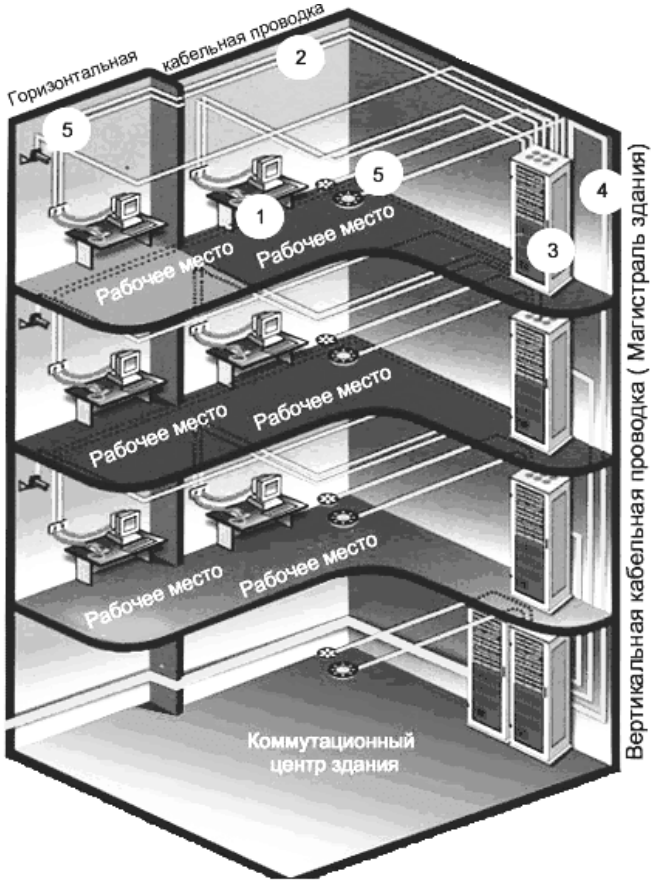

Рисунок 3.8 – Типовая схема размещения коммутационного оборудования в многоэтажном здании

Для организации связи в Центральном офисе понадобится 16 коммутаторов с количеством портов 24, из расчета 1 коммутатор на 1 этаж (так как количество абонентских терминалов на этаже не превышает 24, и

соблюдено условие подключения терминала по витой паре – не более 100 м).

Общее количество требуемого оборудования в филиалах компании сведено в таблицу 3.3

Таблица 3.3 – Результаты расчета объема оборудования

Количество	ЛУАНДА	БЕНГЕЛА	ЗАИР	ЮЖНАЯ КВАНЗА	МАЛАНЖЕ	СЕВЕРНАЯ КВАНЗА
Абонентов	360	312	144	168	216	264
Маршрутизатор для VPN	1	1	1	1	1	1
Коммутаторов	16	14	8	9	11	13
IP PBX	1	1	1	1	1	1

Таким образом, сеть в филиалах компании полностью укомплектована оборудованием, кроме элементов структурированной кабельной системы, которые будут приведены в другом разделе ВКР.

4 РАЗРАБОТКА ТРАНСПОРТНОГО СЕГМЕНТА СЕТИ

Создание собственной транспортной сети обойдется компании Odebrecht слишком дорого или долго. Оптимальным решением в этом случае является создание виртуальной частной сети. Необходимо также обеспечить защиту передаваемых между сегментами сети данных. Возникает проблема, так как у сотрудниковкомпании нет достаточной квалификации для поддержания средств защиты информации, а администратор не может эффективно контролировать все компьютеры во всех сегментах организации.

Кроме того, при защите отдельных каналов инфраструктура корпоративной сети остается прозрачной для внешнего наблюдателя. Для решения этих и некоторых других проблем применяется архитектура VPN, при использовании которой весь поток информации, передаваемый по общедоступным сетям, шифруется с помощью так называемых "канальных шифраторов".

Построение VPN позволяет защитить виртуальную корпоративную сеть так же надежно, как и собственную сеть (а иногда даже и лучше). Данная технология бурно развивается, и в этой области уже предлагаются достаточно надежные решения.

4.1 Организация сети VPN ГК Odebrecht

Цель VPN-технологий состоит в максимальной степени обособления потоков данных одного филиала компании Odebrecht от потоков данных всех других пользователей публичной сети. Обособленность должна быть обеспечена в отношении параметров пропускной способности потоков и в

конфиденциальности передаваемых данных.

В данном проекте VPN будет применяться для решения трех разных задач:

- для организации глобальной связи между филиалами компании Odebrecht (интрасеть),
- для соединения частной сети компании Odebrecht с ее деловыми партнерами и клиентами (экстрасеть),
- для взаимодействия с корпоративной сетью отдельных мобильных пользователей или работающих дома сотрудников (удаленный доступ).

В настоящее время используются различные технологии и архитектуры с учетом потребностей конкретной сети. В качестве среды для создания виртуальных частных сетей выступают сети пакетной коммутации.

4.2 Разработка сценария реализации сети VPN

Существуют разные схемы взаимодействия провайдера и клиента:

- **Пользовательская схема** – оборудование размещается на территории клиента, методы защиты информации и обеспечения QoS организуются самостоятельно.
- **Провайдерская схема** – средства VPN размещаются в сети провайдера, методы защиты информации и обеспечения QoS организуются провайдером.
- **Смешанная схема** – используется при взаимодействии клиента с несколькими провайдерами.

В проекте принято решение использовать провайдерская схема, т.е. механизмы обеспечения безопасности реализуются провайдером – крупнейшим оператором Анголы – «Ангола Телеком», который хорошо

зарекомендовал себя на рынке инфокоммуникаций республики и является надежным партнером.

Типовая схема соединения филиалов с центральным офисом показана на рисунке 4.1.

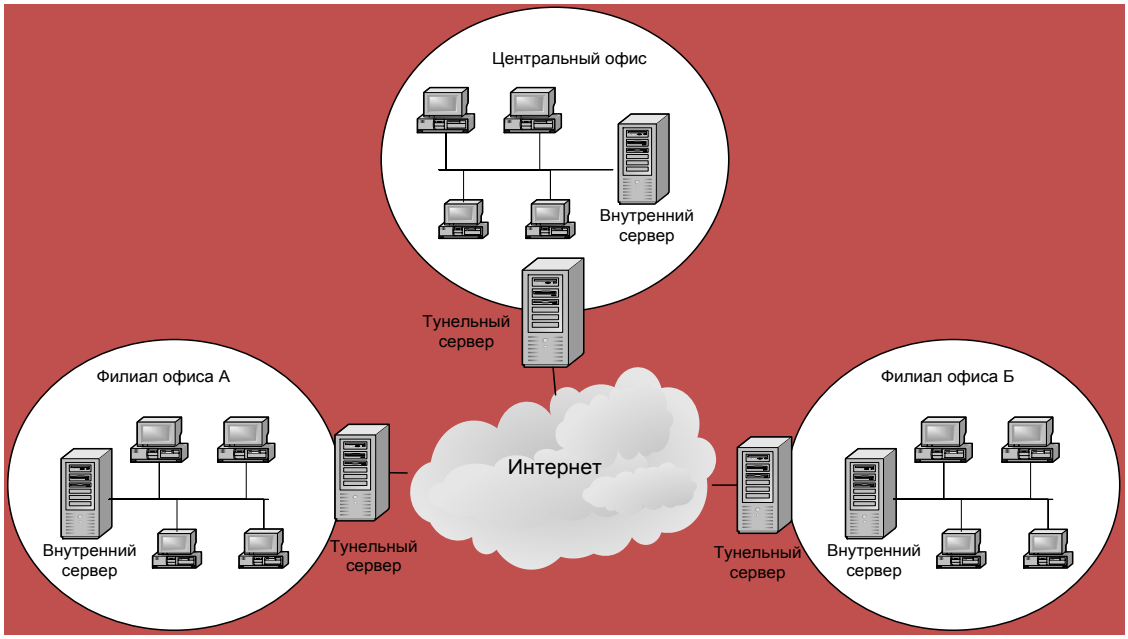

Рисунок 4.1 - Схема соединения филиалов с центральным офисом

Организация туннеля через провайдера Internet, поддерживающего службу VPN, показана на рисунке 4.2.

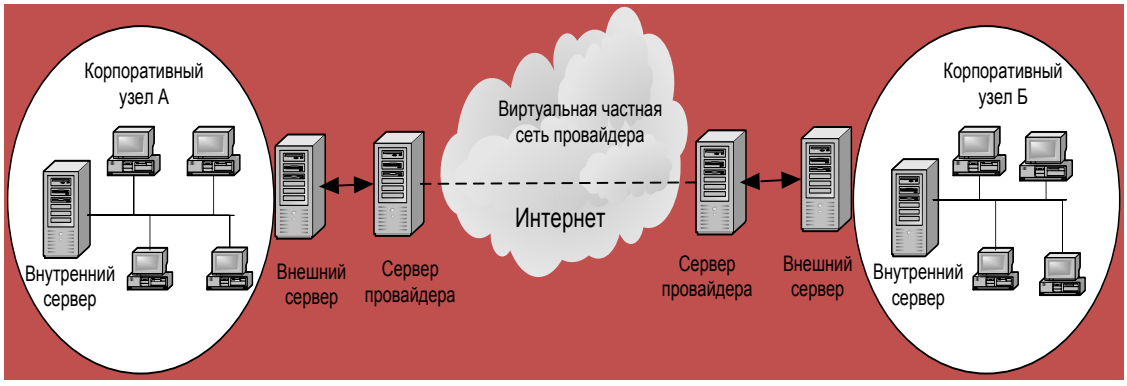

Рисунок 4.2 - Организация туннеля через провайдера Internet, поддерживающего службу VPN

Для того чтобы виртуальные частные сети использовались как полноценный транспорт для передачи трафика, необходимы не только гарантии на качество передачи, но и гарантии в безопасности передаваемых данных. К средствам VPN относится широкий круг устройств безопасности: многофункциональные брандмауэры, маршрутизаторы со встроенными возможностями фильтрации пакетов, proxy-серверы, аппаратные и программные шифраторы передаваемого трафика.

Шлюз VPN – это сетевое устройство, подключенное к нескольким сетям, которое выполняет функции шифрования и аутентификации для многочисленных хостов позади него. Размещение шлюза должно быть аналогично размещению брандмауэра, т.е. таким образом, чтобы через него проходил весь трафик, предназначенный для внутренней корпоративной сети. В зависимости от стратегии безопасности предприятия, исходящие пакеты либо шифруются, либо посылаются в открытом виде, либо блокируются шлюзом. Для входящих туннелируемых пакетов внешний адрес является адресом VPN-шлюза, а внутренний адрес – адресом некоторого хоста позади шлюза. Шлюз VPN может быть реализован всеми перечисленными выше способами, т.е. в виде отдельного аппаратного устройства, отдельного программного решения, а также в виде брандмауэра или маршрутизатора, дополненных функциями VPN.

В качестве Шлюза VPN принято решение использовать маршрутизатор Cisco 2811-SEC/K9. При этом в главном офисе компании г.Луанда будет организован VPN-сервер, а в остальных офисах – VPN-клиент. Для обеспечения информационной безопасности будет приобретена дополнительная опция (поддержка защищенного соединения за счет шифрования) – лицензия для маршрутизатора Cisco 2811/K9: VPN с поддержкой безопасности и шифрования (VPN сервер + VPN клиент, до 10 клиентов). Лицензия оплачивается ежегодно, и учитывается в годовых эксплуатационных расходах.

Основные характеристики [10]

Маршрутизаторы семейства Cico 2800 отличаются увеличенной производительностью, обладают увеличенным объемом памяти, а также новыми интерфейсами высокой плотности. Кроме того, маршрутизаторы семейства Cisco 2800 поддерживают некоторые функции безопасности на аппаратном уровне (2811 Security Bundle,Adv Security,128F/512D).

Особенности:

Маршрутизаторы серии Cisco 2800 поставляются с предустановленным ПО Cisco IOS, и поддерживают концепцию сети с возможностями самозащиты Cisco Self-Defending Network. Маршрутизаторы обладают продвинутыми функциями безопасности и возможности контроля, например, межсетевой экран, аппратное ускорение шифрования данных, поддержку IPSec VPN (с использованием алгоритмов шифрования AES, 3DES, DES), фильтрацию по URL, систему предотвращения вторжений (IPS), контроль доступа к сети (NAC).

Технические характеристики:

- Security Bundle with IOS Advanced Security Image
- WAN/LAN - интерфейсы: 2 x 10/100 Fast Ethernet
- Флеш-память: - по умолчанию: 64 МБ; - максимум: 256 МБ
- Оперативная память: - по умолчанию: 256 МБ; - максимум: 768 МБ
- Слоты расширения: 2 x PVDM (DSP), - 4 x HWIC/VWIC/WIC/VIC-400 Мб/сек (полудуплекс) или 800 Мб/сек (общая), поддержка PoE, - 2 x AIM, - 1 x NM/NME-1.6 Гб/сек и поддержка PoE
- Производительность: 120 000 пакетов/с
- Производительность межсетевого экрана: до 130 Mbps
- Число телефонов в IP АТС CallManager Express или Survivable Remote Site Telephony: до 36 IP-телефонов
- Число одновременных звонков по цифровым каналам: до 80
- Число аналоговых телефоных линий: до 28 FXS или 24 FXO.

В проекте принято решение на базе маршрутизаторов Cisco 2811 SEC/K9 организовать VPN-тоннель, соединяющий филиалы компании, как показано на проектируемой схеме организации транспортной сети на рисунке 4.3.

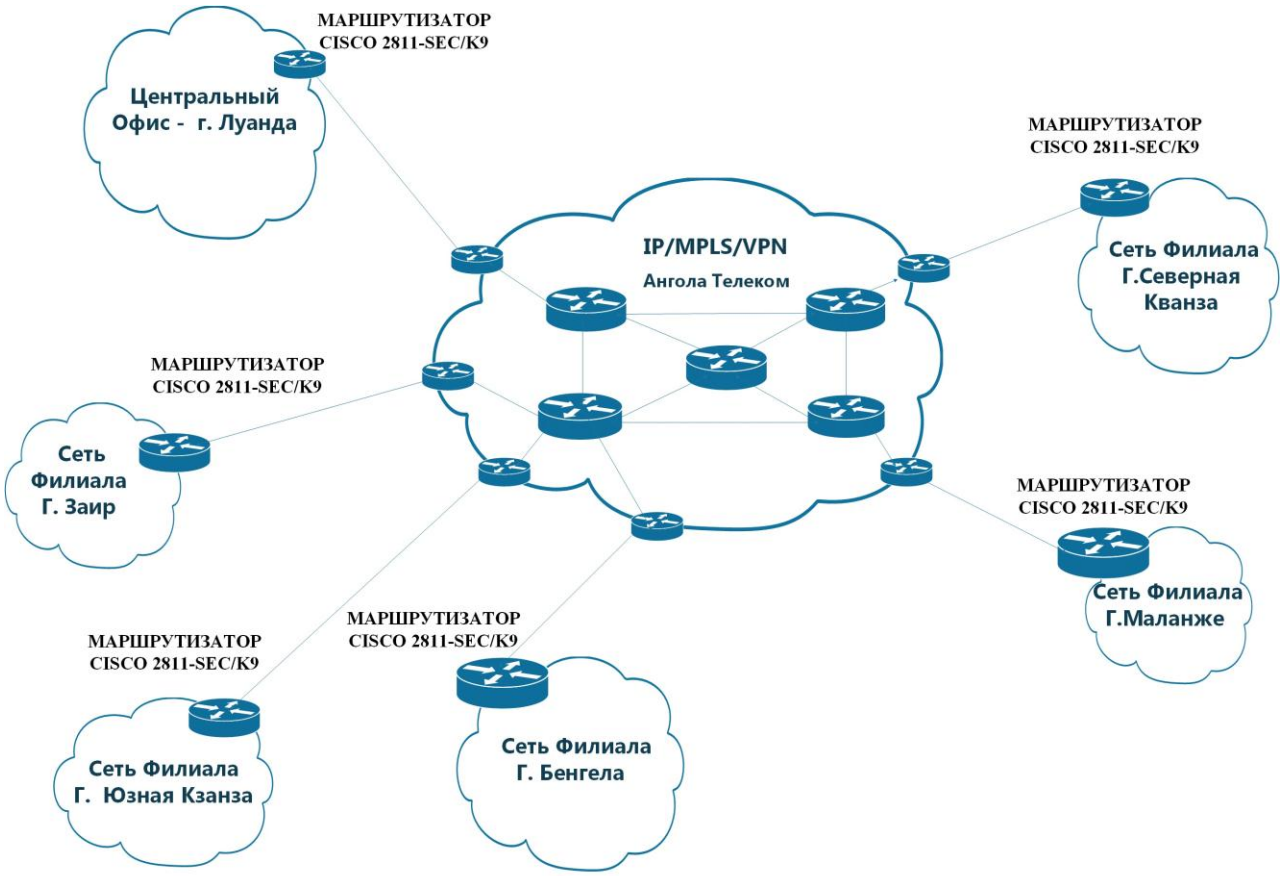

Рисунок 4.3 - Проектируемая схема организации транспортной сети на базе VPN

На транспортном сегменте сети провайдера используется технология MPLS. MPLS VPN делится на две области: сети IP клиентов и внутренняя (магистральная) сеть MPLS провайдера, которая необходима для объединения сетей клиентов (см. рисунок 4.4).

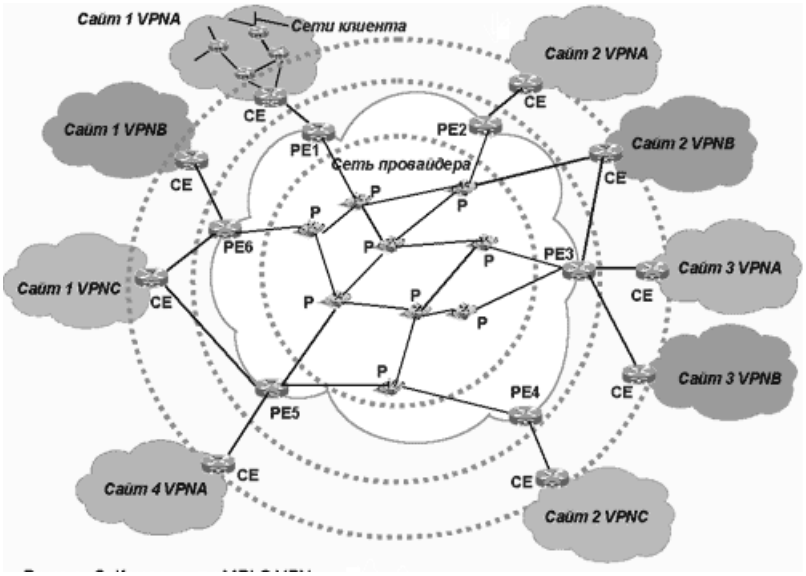

Рисунок 4.4 - Компоненты MPLS VPN

У компании Odebrecht будут созданы территориально обособленные IP-сети, количество которых будет равно количеству филиалов. Каждая из сетей филиалов будет включать несколько подсетей, связанных маршрутизаторами. Такие территориально изолированные сетевые «островки» корпоративной сети принято называть сайтами. Принадлежащие одному клиенту сайты обмениваются пакетами IP через сеть провайдера и образуют виртуальную частную сеть этого клиента. Корпоративная сеть Odebrecht, в которой сеть центрального офиса в Луанде связывается с пятью удаленными филиалами, состоит из шести сайтов. Для обмена маршрутной информацией в пределах сайта узлы пользуются одним из внутренних протоколов маршрутизации (Interior Gateway Protocol, IGP), область действия которого ограничена автономной системой: RIP, OSPF или IS-IS.

Маршрутизатор, с помощью которого сайт клиента подключается к магистрали провайдера, называется пограничным маршрутизатором клиента (Customer Edge router, CE). Будучи компонентом сети клиента, CE ничего не знает о существовании VPN. Он может быть соединен с магистральной сетью провайдера несколькими каналами.

Магистральная сеть провайдера является сетью MPLS, где пакеты IP

продвигаются на основе не IP-адресов, а локальных меток. Сеть MPLS состоит из маршрутизаторов с коммутацией меток (Label Switch Router, LSR), которые направляют трафик по предварительно проложенным путям с коммутацией меток (Label Switching Path, LSP) в соответствии со значениями меток. Устройство LSR своеобразный гибрид маршрутизатора IP и коммутатора, при этом от маршрутизатора IP берется способность определять топологию сети с помощью протоколов маршрутизации и выбирать рациональные пути следования трафика, а от коммутатора — техника продвижения пакетов с использованием меток и локальных таблиц коммутации. В сети провайдера среди устройств LSR выделяют пограничные маршрутизаторы (Provider Edge router, PE), к которым через маршрутизаторы CE подключаются сайты клиентов и внутренние маршрутизаторы магистральной сети провайдера (Provider router, P). Маршрутизаторы CE и PE обычно связаны непосредственно физическим каналом, на котором работает какой-либо протокол канального уровня — например, PPP, FR, ATM или Ethernet. Общение между CE и PE идет на основе стандартных протоколов стека TCP/ IP, поддержка MPLS нужна только для внутренних интерфейсов PE (и всех интерфейсов P). Иногда полезно различать относительно направления продвижения трафика входной PE и выходной (удаленный) PE.

В магистральной сети провайдера только пограничные маршрутизаторы PE должны быть сконфигурированы для поддержки виртуальных частных сетей, поэтому только они «знают» о существующих VPN. Если рассматривать сеть с позиций VPN, то маршрутизаторы провайдера P непосредственно не взаимодействуют с маршрутизаторами заказчика CE, а просто располагаются вдоль туннеля между входным и выходным маршрутизаторами PE.

Маршрутизаторы PE являются функционально более сложными, чем P. На них возлагаются главные задачи по поддержке VPN, а именно

разграничение маршрутов и данных, поступающих от разных клиентов. Маршрутизаторы PE служат также оконечными точками путей LSP между сайтами заказчиков, и именно PE назначает метку пакету IP для его транзита через внутреннюю сеть маршрутизаторов P.

Пути LSP могут быть проложены двумя способами: либо с применением технологии ускоренной маршрутизации (IGP) с помощью протоколов LDP, либо на основе технологии Traffic Engineering с помощью протоколов RSVP или CR-LDP. Прокладка LSP означает создание таблиц коммутации меток на всех маршрутизаторах PE и P, образующих данный LSP. В совокупности эти таблицы задают множество путей для разных видов трафика клиентов.

Несмотря на сложность механизмов MPLS VPN, процесс конфигурирования новой VPN прост, поэтому он хорошо формализуется и автоматизируется. Для исключения возможных ошибок конфигурирования производители разработали автоматизированные программные системы конфигурирования MPLS. Cisco VPN Solution Center снабжает администратора средствами графического интерфейса для формирования состава каждой VPN, а затем переносит полученные конфигурационные данные в маршрутизаторы PE.

Основными преимуществами организации VPN на базе MPLS можно назвать:

- масштабируемость;
- возможность пересечения адресных пространств, узлов подключенных в различные VPN;
- изолирование трафика VPN друг от друга на втором уровне модели OSI.

Масштабируемость достигается за счет того, что подключение нового узла в существующий VPN производиться только перенастройкой одного PE, к которому подключается данный узел.

В различных VPN адресные пространства могут пересекаться, что может быть чрезвычайно полезным, в случае если оператору необходимо предоставить VPN нескольким клиентам, использующим одинаковое приватное адресное пространство, например, адреса 10.0.0.0/8.

Устройства P (LSR) при коммутации анализируют только внешнюю метку, определяющую LSP между PE, и не анализируют заголовок IP пакета, то справедливо говорить о том, что P устройства выполняют функции коммутации на втором уровне модели OSI. Устройства PE так же разделяют маршрутную информацию, таблицы маршрутизации, интерфейсы, направленные в сторону устройств CE, между VRF. Тем самым процессы маршрутизации разных VPN полностью разделяются, и обеспечивается разделение трафика от разных VPN на втором уровне модели OSI. [5,6,7, 10]

4.3 Обеспечение безопасности в сетях MPLS-VPN

Технология MPLS/VPN в реализации компании Cisco Systems обеспечивает такой же уровень безопасности как сети Frame Relay и ATM. Безопасность в сетях MPLS-VPN поддерживается с помощью сочетания протокола BGP и системы разрешения IP-адресов.

BGP-протокол отвечает за распространение информации о маршрутах. Он определяет, кто и с кем может связываться с помощью многопротокольных расширений и атрибутов community. Членство в VPN зависит от логических портов, которые объединяются в сеть VPN и которым BGP присваивает уникальный параметр Route Distinguisher (RD). Параметры RD неизвестны конечным пользователям, и поэтому они не могут получить доступ к этой сети через другой порт и перехватить чужой поток данных. В состав VPN входят только определенные назначенные порты. В сети VPN с функциями MPLS протокол BGP распространяет

таблицы FIB (Forwarding Information Base) с информацией о VPN только участникам данной VPN, обеспечивая таким образом безопасность передачи данных с помощью логического разделения трафика.

Именно провайдер, а не заказчик присваивает порты определенной VPN во время ее формирования. В сети провайдера каждый пакет ассоциирован с RD, и поэтому попытки перехвата пакета или потока трафика не могут привести к прорыву хакера в VPN. Пользователи могут работать в сети интранет или экстранет, только если они связаны с нужным физическим или логическим портом и имеют нужный параметр RD. Эта схема придает сетям Cisco MPLS-VPN очень высокий уровень защищенности.

В опорной сети информация о маршрутах передается с помощью стандартного протокола Interior Gateway Protocol (IGP), такого как OSPP или IS-IS. Пограничные устройства PE в сети провайдера устанавливают между собой связи-пути, используя LDP для назначения меток.

Назначения меток для внешних (пользовательских) маршрутов распространяется между PE-маршрутизаторами не через LDP, а через многопротокольные расширения BGP. Атрибут Community BGP ограничивает рамки информации о доступности сетей и позволяет поддерживать очень крупные сети, не перегружая их информацией об изменениях маршрутной информации. BGP не обновляет информацию на всех периферийных устройствах PE, находящихся в провайдерской сети, а приводит в соответствие таблицы PIB только тех PE, которые принадлежат к конкретной VPN.

Если виртуальные каналы создаются при оверлейной модели, исходящий интерфейс любого индивидуального пакета данных является функцией только входящего интерфейса. Это означает, что IP-адрес пакета не определяет маршрута его передачи по магистральной сети. Это позволяет предотвратить попадание несанкционированного трафика в сеть VPN и

передачу несанкционированного трафика из нее.

В сетях MPLS-VPN пакет, поступающий в магистраль, в первую очередь ассоциируется с конкретной сетью VPN на основании того, по какому интерфейсу (подин-терфейсу) пакет поступил на PE-маршрутизатор. Затем IP-адрес пакета сверяется с таблицей передачи (forwarding table) данной VPN. Указанные в таблице маршруты относятся только к VPN принятого пакета. Таким образом, входящий интерфейс определяет набор возможных исходящих интерфейсов. Эта процедура также предотвращает как попадание несанкционированного трафика в сеть VPN, так и передачу несанкционированного трафика из нее. [20 ,22 ,23]

4.4 Обеспечение физического соединения с сетью провайдера

В качестве провайдера выбран Оператор связи Ангола – Телеком. От точки доступа к сети провайдера (здания АТС), до центрального офиса компании Odebrecht в Луанде, будет проложен волоконно-оптический кабель в свободном канале существующей телефонной кабельной канализации.

Схема трассы кабельной линии показана на рисунке 4.5.

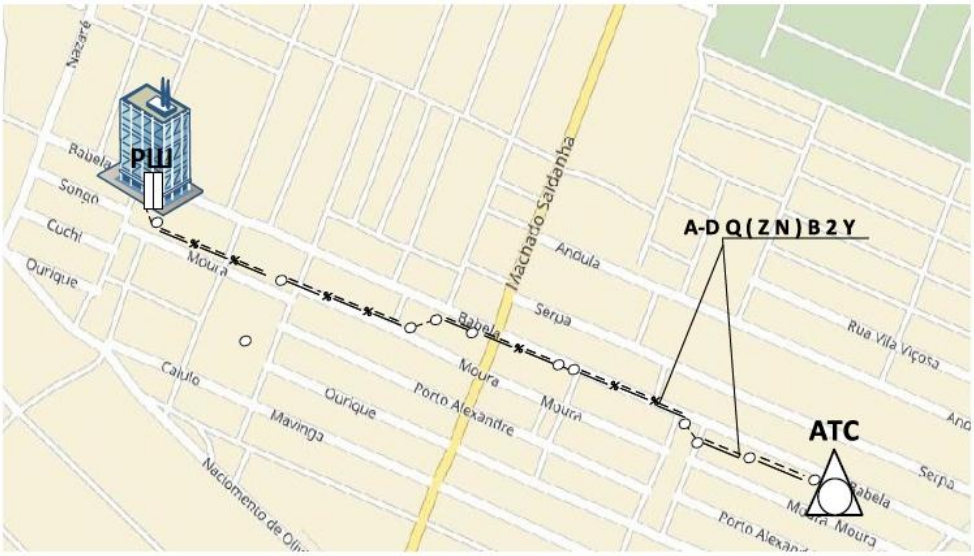

Рисунок 4.5 – Проектируемая схема трассы прокладки кабеля

Принято решение использовать кабель модели HELUCOM® pact немецкого производста фирмы Helukabel, т.к. он уже применяется операторами связи в Анголе (Ангола Телеком).

Выбран оптический кабель марки A-DQ(ZN)B2Y, central, Helukom: Кабель волоконно-оптический, с центральным модулем, наружный, Helukabel. Оптический кабель A-DQ(ZN)B2Y предназначен для использования внутри объекта, прокладки в телефонной кабельной канализации или же в специально предназначенных пластиковых трубах. Рабочая температура эксплуатации кабеля составляет −20 до +60 градусов.

Рисунок 4.6 – Кабель оптический A-DQ(ZN)B2Y

В центре кабеля расположен модуль оптический, с количеством одномодовых оптических волокон – 8, кабель усилен арамидными нитями, обеспечивающими защиту от грызунов, разгрузку от натяжения и продольную водостойкость кабеля. На внешней оболочке тиснением показана марка. [13, 14]

5 РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО РЕАЛИЗАЦИИ ИНФОКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ ГК ODEBRECHT

5.1 Рекомендации по размещению оборудования

5.1.1 Серверная

Для размещения оборудования в здании офиса выделено отдельное помещение – серверная. В серверной будут установлены стойки с оборудованием IP PBX (узел агрегации), шлюзы, серверная платформа, маршрутизатор, а также расположено оборудование для электропитания и заземления. Кроме того, в помещении необходимо обеспечить требуемый микроклимат, т.е. система кондиционирования и вентиляции. В примыкающем помещении будет находиться рабочее место инженера – администратора сети. Проектируемые схемы размещения оборудования показаны на рисунках 5.1 и 5.2.

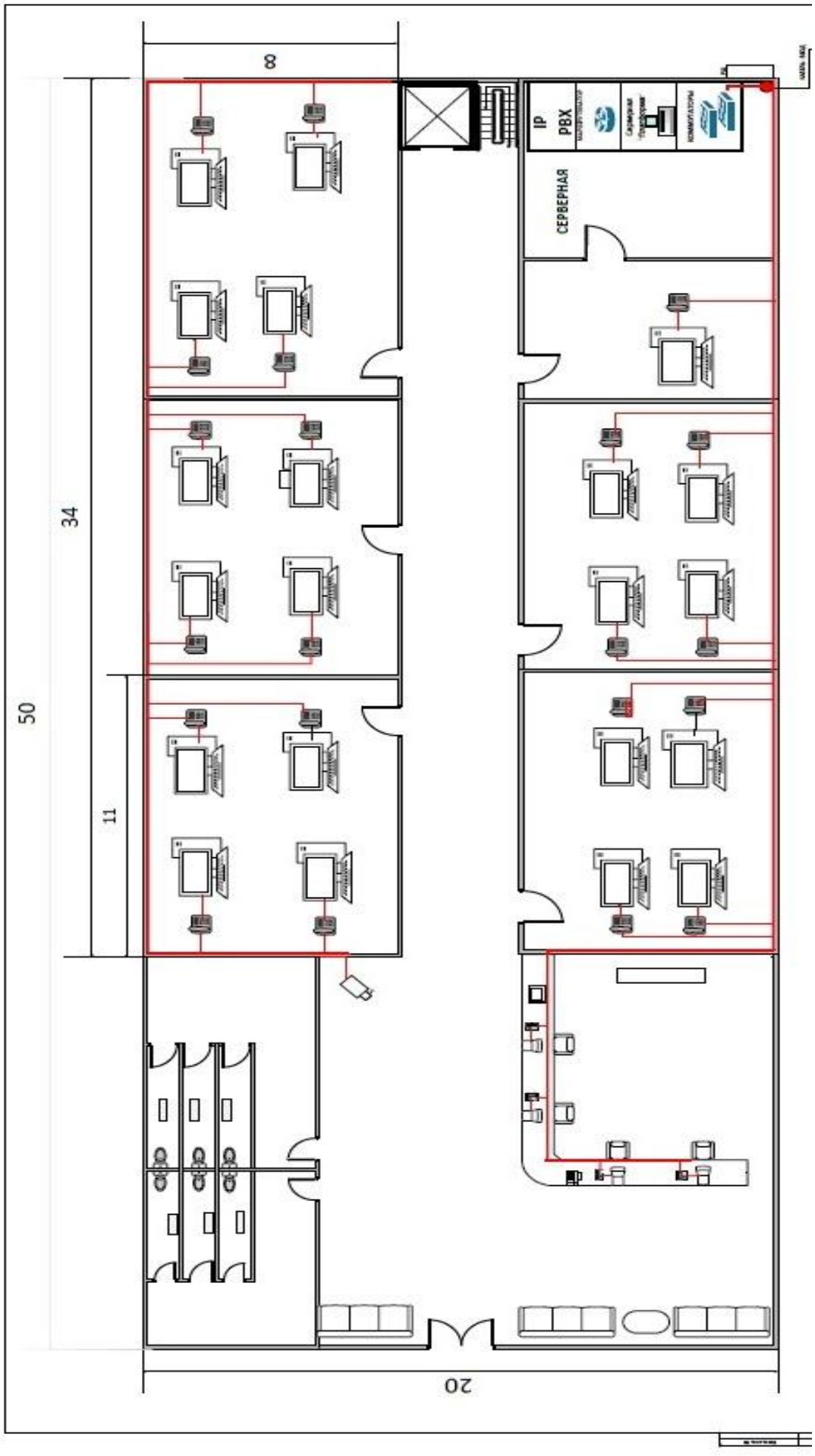

Рисунок 5.1 – Проектируемая схема размещения оборудования на 1 этаже Центрального офиса г.Луанда

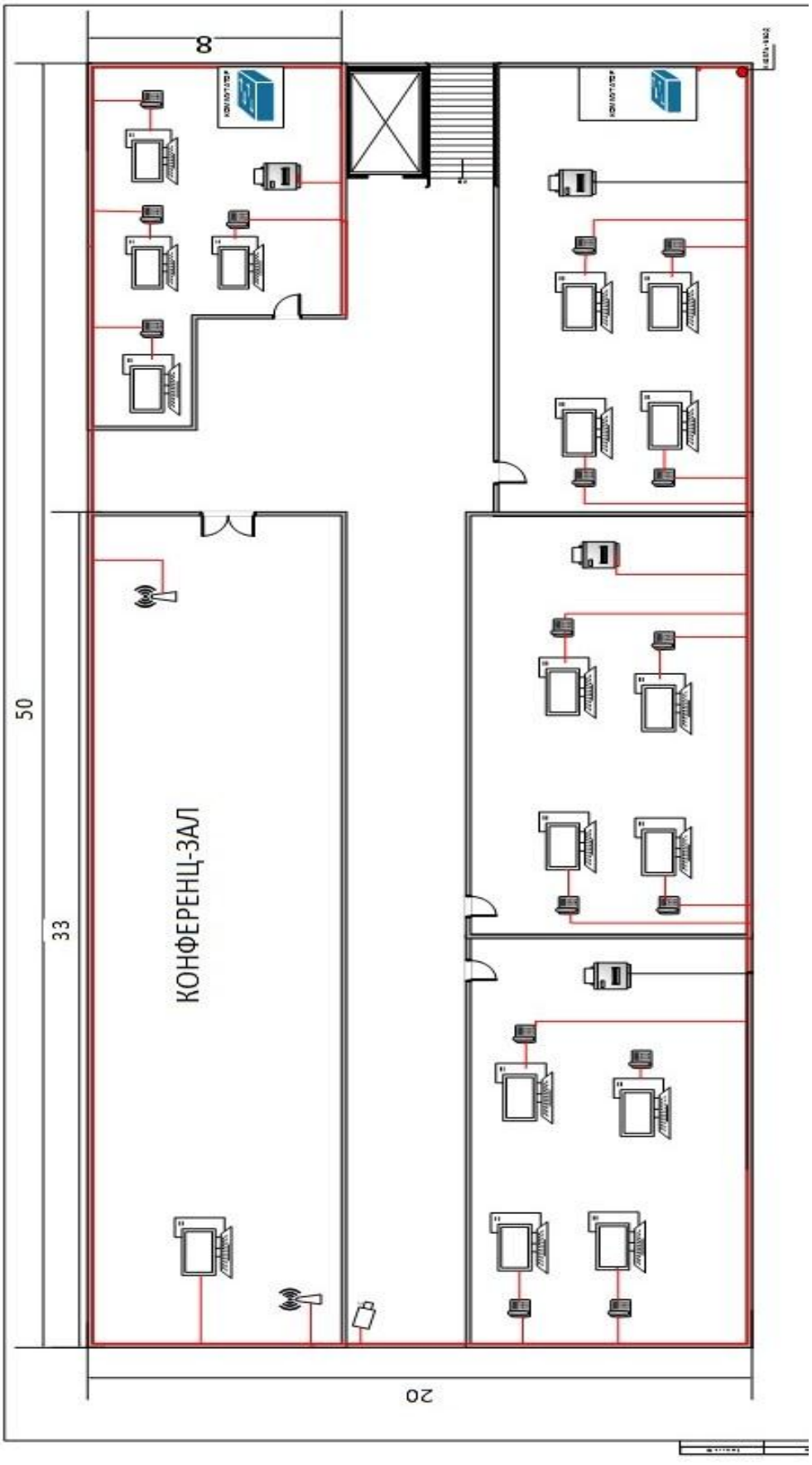

Рисунок 5.2 – Проектируемая схема размещения оборудования на верхнем этаже Центрального офиса г.Луанда

5.1.2 Структурированная кабельная система офисного здания в г.Луанда

От серверной по кабель-каналам будет проводиться разводка горизонтальных и вертикальных кабельных подсистем СКС, посредством которых будет обеспечено подключение коммутаторов доступа на этажах здания. Вертикальны Кабель-канал будет проходить по стене серверной, снизу, от места ввода магистрального кабеля, вверх – через межэтажные перегородки до верхнего этажа. В вертикальной подсистеме кабельных магистралей будет проложен волоконно-оптический кабель, соединяющий коммутатор агрегации с коммутаторами доступа на каждом этаже.

Горизонтальная подсистема предназначена для организации прокладки кабеля UTP cat 5e, соединяющего коммутаторы доступа с оконечными устройствами – телефонами и компьютерами. В горизонтальной подсистеме, кроме кабель-каналов, будут использованы розетки, адаптеры, шнуры. Для пользователя в помещении офиса будет предусмотрена подсистема рабочего места. Полный перечень элементов СКС представлен в таблице 5.1.

Таблица 5.1 – Состав СКС в Центральном офисе г.Луанда

Наименование и техническая характеристика	Ед. изм.	Кол-во
IP PBX Cisco Business Edition 6000 (лицензия на 15534 портов)	шт	1
Серверная платформа	шт	1
Маршрутизатор Cisco 2811/K9	шт	1
Коммутатор (switch) Cisco WS-C2960G-24TC-L	шт	16
IP-телефон Cisco CP-7962G	шт	360
Кабель витая пара 5-ой категории, м	м	7 940
Соединительный кабель MDF, метров	м	370
Розеточный модуль категории 5e серии MAX, 1-портовый, T568B, наклонный	шт	370
Адаптер 45x45 мм для установки розеточных модулей	шт	360
Оконечные шнуры с модульными разъемами RJ45, категория 5e, длина 2 м	шт	180

Окончание таблицы 5.1

Наименование и техническая характеристика	Ед. изм.	Кол-во
Оконечные шнуры с модульными разъемами RJ45, категория 5e, длина 3 м	шт	180
Кабель оптический: 12 x 62,5/125 волокна в PVC оболочке .	м	65
Коммутационный шнур с разъемами 110-110, 1 пара - 1,0 м	шт	360
Монтажное оборудование	шт	4
Шкаф напольный 42 U, 2033x800x875 мм	шт	1
Комплект для соединения шкафов	шт	1
Модуль вентиляторный 600 Series (монтаж сверху) - 2 вентилятора	шт	1
Комплект для заземления	шт	1
Полка, перфорированная для оборудования 19" длиной 454 мм	шт	1
Силовые розетки для шкафов, вертикальные, 8 розеток	шт	2

В остальных офисах планирование СКС проведено аналогично. В результате для технико-экономического обоснования проведено определение стоимости работ, включая оборудование и материалы, в пересчёте на 1 рабочее место, что составило 6500 руб. на абонента. Стоимость горизонтальных и вертикальных подсистем СКС зависит от протяженности кабельных магистралей и количества компонентов. Воспользовавшись калькулятором СКС [30] определена стоимость реализации СКС в каждом филиале, результат приведен в смете затрат на приобретение оборудования раздела ТЭО.

5.2 Охрана труда, экологическая безопасность проекта

Все оборудование, применяемое в сети, имеет сертификат и разрешено для использования на территории Республики Ангола.

Специалисты, эксплуатирующие оборудование, находятся за рабочим местом, т.е. компьютером. Отрицательное воздействие на человека вычислительной техники выражается нарушением функций зрения,

быстрым общим утомлением, заболеваниями нервной системы, раком и прочими отрицательными явлениями у людей, длительное время использующих дисплеи при несоблюдении эргономических требований.

С точки зрения эргономики группа требований при работе с ЭВМ включает требования к функциональным помещениям и к факторам внешней среды, которые в свою очередь подразделяются соответственно на требования к объему и форме рабочего помещения, обеспечивающим вход и выход, перемещение внутри помещения, и требования к физическим, химическим и биологическим факторам внешней среды, а также к электрической и пожарной безопасности. В проекте предусмотрена отдельная комната для размещения сетевого оборудования – серверная. Обслуживающий сеть персонал находится в соседнем помещении, и не подвергается постоянному воздействию возможных электро-магнитных полей.

Основные требования к учету факторов рабочей среды заключаются в том, что они при их комплексном воздействии на человека не должны оказывать отрицательного влияния на его здоровье при профессиональной деятельности в течение длительного времени, и кроме того, не должны вызывать снижения надежности и качества деятельности оператора при воздействии в течении рабочей смены. При анализе влияния факторов рабочей среды на человека-оператора различают четыре уровня их воздействия: комфортная рабочая среда, когда величины факторов среды не превышают требований нормативно-технических документов, относительно дискомфортная рабочая среда, когда в рабочей зоне отдельные производственные факторы несколько превышают предельно допустимый уровень, экстремальная рабочая среда и сверхэкстремальная рабочая среда.

Для того чтобы организовать комфортную среду при работе с персональным компьютером, необходимо изучить требования к ней, регламентированные соответствующими нормативно-техническими

документами, и возможные средства и способы защиты от неблагоприятных факторов в случае превышения в реальности нормированных величин.

Одним из важных факторов, которые влияют на работоспособность и состояние здоровья пользователей ПЭВМ, является организация рабочего места. Неправильная организация рабочего места приводит к общей усталости, головным болям, усталости мышц рук, болям в спине и шее.

Такие негативные моменты чаще всего возникают из-за несоответствия помещений и организации рабочих мест эргономическим требованиям и санитарно-производственным нормам.

Общие эргономические требования для организации рабочего места

Параметры рабочего места должны быть следующими. Площадь аудитории, в которой будет проходить работа должна быть не менее 6 $м^2$, а объем не менее 24 $м^3$. Для внутренней отделки помещения должны использоваться диффузно-отражающие материалы с коэффициентом отражения для потолка - 0,7-0,8; для стен - 0,5-0,6; для пола - 0,3-0,5.

Конструкция рабочего стола должна обеспечивать оптимальное размещение на рабочей поверхности используемого оборудования. Конструкция рабочего стула (кресла) должна обеспечивать поддержание рациональной рабочей позы при работе с видео-дисплейным терминалом и ПЭВМ, позволять изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления работающего. Поверхность сиденья, спинки и других элементов стула (кресла) должна быть полумягкой, с нескользящим, не электризующимся и воздухонепроницаемым покрытием, обеспечивающим легкую очистку от загрязнения.

Рабочий стол должен иметь пространство для ног высотой не менее 600 мм, шириной - не менее 500 мм, не менее 450 мм в глубину на уровне колен и на уровне вытянутых ног – не менее 650 мм. Рабочее место должно

быть оборудовано подставкой для ног, имеющей ширину не менее 300 мм, глубину не менее 400 мм, регулировку по высоте в пределах 150 мм по углу наклона опорной поверхности подставки до 20 градусов.

Расстояние от глаз пользователя до экрана дисплея должно составлять 500-700 мм. Угол зрения 10-20°, но не более 40°; угол между верхним краем дисплея и уровнем глаз пользователя должен составлять не менее 10°. Предпочтительным является расположение экрана перпендикулярно к линии зрения пользователя.

Рабочие места по отношению к световым проемам должны располагаться не ближе 3 м так, чтобы естественный свет падал сбоку, преимущественно слева.

Освещенность также влияет на состояние здоровья и работоспособность человека. В данном случае пользователь будет работать за дисплеем и, а особенностью такой работы является постоянное и значительное напряжение функций зрительного анализатора, обусловленного необходимостью различения самосветящихся объектов (символов, знаков) при наличии бликов на экране, строчной структурой экрана, мельканием изображения, не достаточной четкостью объектов различения. Для того чтобы избежать перенапряжения и болей в глазах, установлены специальные гигиенические нормы производственного освещения.

На сегодняшний день для повышения комфорта работы с ПК и уменьшения его влияния на здоровье оператора необходим правильный выбор монитора. У большинства современных мониторов для снижения интенсивности бликов, возникающих в результате отражения света от внешних источников, на экран нанесено специальное покрытие. Чем более плоский экран у кинескопа, тем легче избавится от бликов, повернув или наклонив экран (у мониторов с трубкой Trinitron практически абсолютно плоский экран). Исходя из сказанного выше можно сделать вывод, что чем

качественнее используемая вычислительная техника и чем более скрупулезно учтены условия внешней среды, тем больше шансов у человека сохранить собственное здоровье.

Излучения ПК могут быть опасными для здоровья. Низкочастотные поля при продолжительном облучении сидящих у ПК людей могут привести к нарушениям самых различных физиологических процессов. Мощность дозы рентгеновского излучения в любой точке пространства на расстоянии 5 см от экрана видеомонитора при 41 часовой рабочей неделе не должна превышать 100 мкР/ч (0,03 мкР/с), а интенсивность ультрафиолетового излучения — 10 Вт/м2 .

Высокая температура воздуха отрицательно сказывается на функциональном состоянии человека. Все основные электронные блоки ПК имеют встроенные вентиляторы для обеспечения стабильных температурных режимов их функционирования, поэтому при создании комфортных условий работы особое внимание необходимо уделить путям отвода воздуха (приточно-вытяжной вентиляции).

В проекте сети ГК Odebrecht для оптимизации среды обитания оператора персонального компьютера организован комфортный микроклимат на рабочем месте. В этих целях рекомендовано применить встроенные кондиционеры для динамического изменения микроклимата, а также вентиляторы. В помещении, где работает оператор компьютера, желательно подобрать цветовую гамму поверхностей таким образом, чтобы добиться оптимального отдыха зрения. Для исключения дискомфортных зрительных условий, вызванных влиянием внешней среды, на окнах помещений применяют шторы или жалюзи. Снижение уровня шума можно добиться применением звукопоглощающих материалов. Кроме того, предусмотрено отдельное помещение для размещения оборудования (серверная), где оператор будет находиться кратковременно, только для работ по техническому обслуживанию. Настройка оборудования будет

производиться дистанционно, с помощью ПК. [12]

5.3 Создание имитационной модели сети ГК Odebrecht

Для анализа созданной архитектуры создана модель сети связи ГК Odebrecht в программной средеCisco Packet Tracer.

Модель представлена на рисунке 5.3.

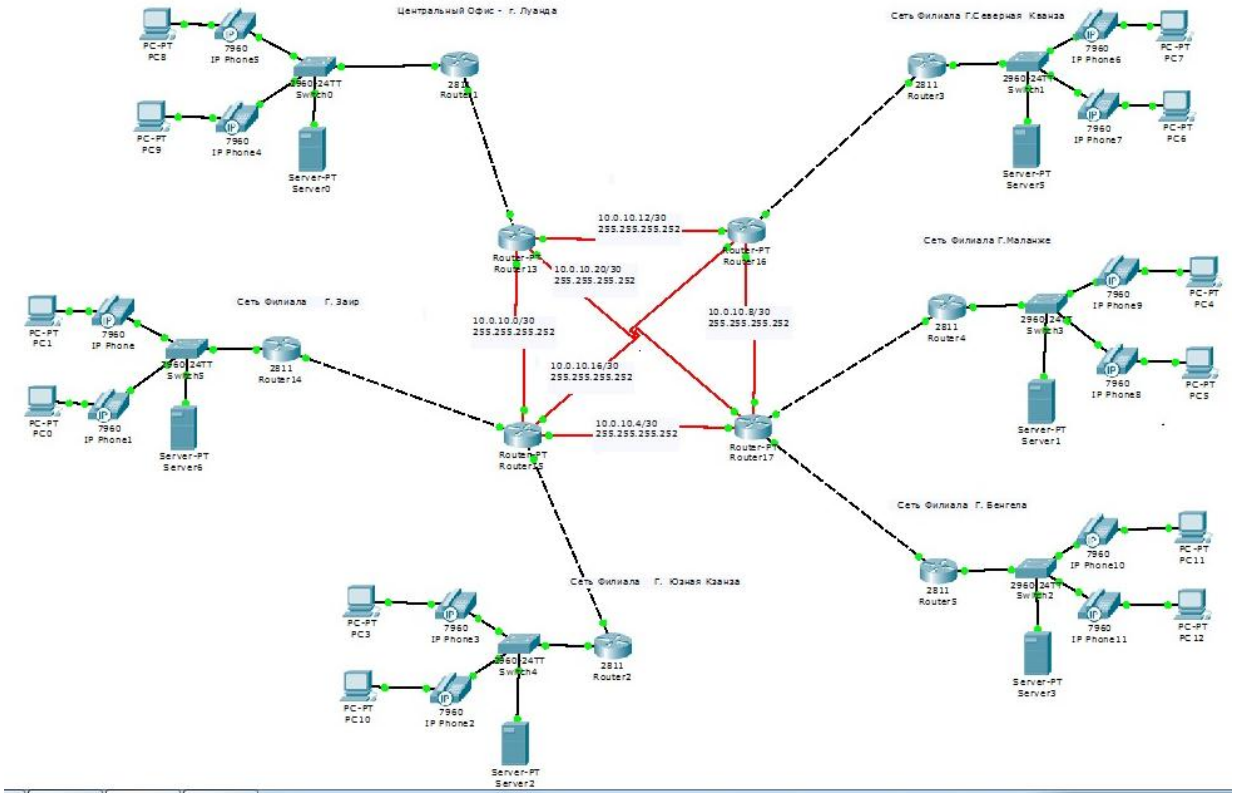

Рисунок 5.3 – Модель проектируемой сети

При создании модели были настроены все сетевые компоненты, и проверена работа сети. Методом пингования отслежены все связи в сетевых сегментах.

При настройке сетей IP-телефонии, реализованных на АТС фирмы Cisco, принято создавать отдельные vlan для голосового трафика и трафика данных.

6 ТЕХНИКО-ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ ПРОЕКТА

6. 1 Расчет капитальных вложений

Капитальные вложения представляют собой смету затрат на реализацию проекта и включают в себя все необходимое коммуникационное оборудование (АТС, коммутаторы, маршрутизаторы, элементы СКС и т.п.), линию связи, единоразовую стоимость лицензионного программного обеспечения и т.д.

Общие капитальные вложения на приобретение оборудования могут быть вычислены по формуле:

$$K_{об} = \sum_{i=1}^{N} K_i, \text{ руб} \qquad (6.1)$$

где $К_{об}$ - суммарный объем затрат на приобретение оборудования, руб; Кi – общая стоимость одной позиции (типа оборудования); N – количество позиций.

Смета затрат представлена в виде таблицы 6.1.

Таблица 6.1 – Смета затрат на приобретение оборудования

Наименование	Кол-во единиц	Стоимость (руб)	
		за единицу	всего
Центральный офис г.Луанда			
IP PBX Cisco Business Edition 6000	1	394 800	394 800
Серверная платформа Cisco Unified Computing System UCSC-C240-M4S, включая лицензии	1	195 525	195 525
Межсетевой экран CISCO ASA5505-K8 ASA 5505 Appliance with SW	1	20 005	20 005
Маршрутизатор Cisco 2811/K9 (VPN сервер)	1	158 000	158 000
Коммутатор (switch) Cisco WS-C2960G-24TC-L	16	58 249	931 984
Кабель оптический транспортного сегмента сети, км	1	5800	5800

Продолжение таблицы 6.1

Наименование	Кол-во единиц	Стоимость (руб)	
		за единицу	всего
IP-телефон Cisco CP-7962G	360	5 451	1 962 360
Кабель витая пара 5-ой категории, м	7 940	9	71 460
Соединительный кабель MDF, метров	20	150	3000
Розеточный модуль категории 5e серии MAX, 1-портовый, T568B, наклонный	370	330	122 100
Адаптер 45x45 мм для установки розеточных модулей	360	136	48 960
Оконечные шнуры с модульными разъемами RJ45, категория 5e, длина 2 м	180	49	8 820
Оконечные шнуры с модульными разъемами RJ45, категория 5e, длина 3 м	180	58	10 440
Кабель оптический: 12 x 62,5/125 волокна в PVC оболочке .м	65	85	5 525
Коммутационный шнур с разъемами 110-110, 1 пара - 1,0 м	360	134	48 240
Монтажное оборудование	4	3 500	14 000
Шкаф напольный 42 U, 2033x800x875 мм	1	32 122	32 122
Комплект для соединения шкафов	1	7 222	7 222
Модуль вентиляторный 600 Series (монтаж сверху) - 2 вентилятора	1	4 700	4 700
Комплект для заземления	1	438	438
Полка перфорированная для оборудования 19" длиной 454 мм	1	1 030	1 030
Силовые розетки для шкафов, вертикальные, 8 розеток	2	2 160	4 320
Итого по офису г.Луанда…			4.050.851
Офис г.Бенгела			
IP PBX Cisco Business Edition 6000	1	394800	394800
Серверная платформа Cisco Unified Computing System UCSC-C240-M4S, включая лицензии	1	195 525	195 525
Межсетевой экран CISCO ASA5505-K8 ASA 5505 Appliance with SW	1	20 005	20 005
Маршрутизатор Cisco 2811/K9 (VPN-клиент)	1	158 000	158 000
Коммутатор (switch) Cisco WS-C2960G-24TC-L	13	58 249	757 237
Кабель оптический транспортного сегмента сети, км	1	5800	5800
IP-телефон Cisco CP-7962G	312	5 451	1 700 712

Продолжение таблицы 6.1

Наименование	Кол-во единиц	Стоимость (руб)	
		за единицу	всего
Кабель витая пара 5-ой категории, м	6 884	9	41 304
Соединительный кабель MDF, метров	20	150	3000
Розеточный модуль категории 5e серии MAX, 1-портовый, T568B, наклонный	320	330	105 600
Адаптер 45x45 мм для установки розеточных модулей	312	136	42 432
Оконечные шнуры с модульными разъемами RJ45, категория 5e, длина 2 м	156	49	7 176
Оконечные шнуры с модульными разъемами RJ45, категория 5e, длина 3 м	156	58	9 048
Кабель оптический: 12 x 62,5/125 волокна в PVC оболочке .м	55	85	4 675
Коммутационный шнур с разъемами 110-110, 1 пара - 1,0 м	312	134	41 808
Монтажное оборудование	4	3 500	14 000
Шкаф напольный 42 U, 2033x800x875 мм	1	32 122	32 122
Комплект для соединения шкафов	1	7 222	7 222
Модуль вентиляторный 600 Series (монтаж сверху) - 2 вентилятора	1	4 700	4 700
Комплект для заземления	1	438	438
Полка перфорированная для оборудования 19" длиной 454 мм	1	1 030	1 030
Силовые розетки для шкафов, вертикальные, 8 розеток	2	2 160	4 320
Итого по офису г. *Бенгела …*			3.550.954
Офис г. ЗАИР			
IP PBX Cisco Business Edition 6000	1	394800	394800
Серверная платформа Cisco Unified Computing System UCSC-C240-M4S, включая лицензии	1	195 525	195 525
Межсетевой экран CISCO ASA5505-K8 ASA 5505 Appliance with SW	1	20 005	20 005
Маршрутизатор Cisco 2811/K9 (VPN-клиент)	1	158 000	158 000
Коммутатор (switch) Cisco WS-C2960G-24TC-L	6	58 249	349 494
Кабель оптический транспортного сегмента сети, км	1	5800	5800
IP-телефон Cisco CP-7962G	144	5 451	784 944
Кабель витая пара 5-ой категории, м	3 188	9	28 692
Соединительный кабель MDF, метров	20	150	3000
Розеточный модуль категории 5e серии MAX, 1-портовый, T568B, наклонный	144	330	47 520

Продолжение таблицы 6.1

Наименование	Кол-во единиц	Стоимость (руб)	
		за единицу	всего
Адаптер 45х45 мм для установки розеточных модулей	144	136	19 584
Оконечные шнуры с модульными разъемами RJ45, категория 5е, длина 2 м	72	49	3 528
Оконечные шнуры с модульными разъемами RJ45, категория 5е, длина 3 м	72	58	4 176
Кабель оптический: 12 х 62,5/125 волокна в PVC оболочке .м	24	85	2 040
Коммутационный шнур с разъемами 110-110, 1 пара - 1,0 м	72	134	9 648
Монтажное оборудование	4	3 500	14 000
Шкаф напольный 42 U, 2033х800х875 мм	1	32 122	32 122
Комплект для соединения шкафов	1	7 222	7 222
Модуль вентиляторный 600 Series (монтаж сверху) - 2 вентилятора	1	4 700	4 700
Комплект для заземления	1	438	438
Полка перфорированная для оборудования 19" длиной 454 мм	1	1 030	1 030
Силовые розетки для шкафов, вертикальные, 8 розеток	2	2 160	4 320
Итого по офису г. *ЗАИР* …			2.090.588
Офис г. ЮЖНАЯ КВАНЗА			
IP PBX Cisco Business Edition 6000	1	394800	394800
Серверная платформа Cisco Unified Computing System UCSC-C240-M4S, включая лицензии	1	195 525	195 525
Межсетевой экран CISCO ASA5505-K8 ASA 5505 Appliance with SW	1	20 005	20 005
Маршрутизатор Cisco 2811/K9 (VPN-клиент)	1	158 000	158 000
Коммутатор (switch) Cisco WS-C2960G-24TC-L	7	58 249	349 494
Кабель оптический транспортного сегмента сети, км	1	5800	5800
IP-телефон Cisco CP-7962G	168	5 451	915 768
Кабель витая пара 5-ой категории, м	3 716	9	33 444
Соединительный кабель MDF, метров	20	150	3000
Розеточный модуль категории 5е серии MAX, 1-портовый, T568B, наклонный	168	330	55 440
Адаптер 45х45 мм для установки розеточных модулей	168	136	22 848

Продолжение таблицы 6.1

Наименование	Кол-во единиц	Стоимость (руб)	
		за единицу	всего
Оконечные шнуры с модульными разъемами RJ45, категория 5е, длина 2 м	84	49	4 116
Оконечные шнуры с модульными разъемами RJ45, категория 5е, длина 3 м	84	58	4 872
Кабель оптический: 12 х 62,5/125 волокна в PVC оболочке .м	28	85	2 380
Коммутационный шнур с разъемами 110-110, 1 пара - 1,0 м	72	134	9 648
Монтажное оборудование	4	3 500	14 000
Шкаф напольный 42 U, 2033х800х875 мм	1	32 122	32 122
Комплект для соединения шкафов	1	7 222	7 222
Модуль вентиляторный 600 Series (монтаж сверху) - 2 вентилятора	1	4 700	4 700
Комплект для заземления	1	438	438
Полка перфорированная для оборудования 19" длиной 454 мм	1	1 030	1 030
Силовые розетки для шкафов, вертикальные, 8 розеток	2	2 160	4 320
Итого по офису г *ЮЖНАЯ КВАНЗА* …			2.238.972
Офис г. Маланже			
IP PBX Cisco Business Edition 6000	1	394800	394800
Серверная платформа Cisco Unified Computing System UCSC-C240-M4S, включая лицензии	1	195 525	195 525
Межсетевой экран CISCO ASA5505-K8 ASA 5505 Appliance with SW	1	20 005	20 005
Маршрутизатор Cisco 2811/K9 (VPN-клиент)	1	158 000	158 000
Коммутатор (switch) Cisco WS-C2960G-24TC-L	9	58 249	524 241
Кабель оптический транспортного сегмента сети, км	1	5800	5800
IP-телефон Cisco CP-7962G	216	5 451	1 177 416
Кабель витая пара 5-ой категории, м	4 772	9	33 444
Соединительный кабель MDF, метров	20	150	3000
Розеточный модуль категории 5е серии MAX, 1-портовый, T568B, наклонный	216	330	71 280
Адаптер 45х45 мм для установки розеточных модулей	216	136	35 208
Оконечные шнуры с модульными разъемами RJ45, категория 5е, длина 2 м	108	49	5 292

Продолжение таблицы 6.1

Наименование	Кол-во единиц	Стоимость (руб)	
		за единицу	всего
Оконечные шнуры с модульными разъемами RJ45, категория 5е, длина 3 м	108	58	6 264
Кабель оптический: 12 х 62,5/125 волокна в PVC оболочке .м	36	85	3 060
Коммутационный шнур с разъемами 110-110, 1 пара - 1,0 м	108	134	14 472
Монтажное оборудование	4	3 500	14 000
Шкаф напольный 42 U, 2033х800х875 мм	1	32 122	32 122
Комплект для соединения шкафов	1	7 222	7 222
Модуль вентиляторный 600 Series (монтаж сверху) - 2 вентилятора	1	4 700	4 700
Комплект для заземления	1	438	438
Полка перфорированная для оборудования 19" длиной 454 мм	1	1 030	1 030
Силовые розетки для шкафов, вертикальные, 8 розеток	2	2 160	4 320
Итого по офису г. *Маланже* …			2.711.639
Офис г. СЕВЕРНАЯ КВАНЗА			
IP PBX Cisco Business Edition 6000	1	394800	394800
Серверная платформа Cisco Unified Computing System UCSC-C240-M4S, включая лицензии	1	195 525	195 525
Межсетевой экран CISCO ASA5505-K8 ASA 5505 Appliance with SW	1	20 005	20 005
Маршрутизатор Cisco 2811/K9 (VPN-клиент)	1	158 000	158 000
Коммутатор (switch) Cisco WS-C2960G-24TC-L	11	58 249	640 739
Кабель оптический транспортного сегмента сети, км	1	5800	5800
IP-телефон Cisco CP-7962G	264	5 451	1 439 064
Кабель витая пара 5-ой категории, м	5 828	9	33 444
Соединительный кабель MDF, метров	20	150	3000
Розеточный модуль категории 5е серии MAX, 1-портовый, T568B, наклонный	264	330	87 120
Адаптер 45х45 мм для установки розеточных модулей	264	136	35 904
Оконечные шнуры с модульными разъемами RJ45, категория 5е, длина 2 м	132	49	6 468
Оконечные шнуры с модульными разъемами RJ45, категория 5е, длина 3 м	132	58	7 656

Окончание таблицы 6.1

Наименование	Кол-во единиц	Стоимость (руб)	
		за единицу	всего
Кабель оптический: 12 х 62,5/125 волокна в PVC оболочке .м	44	85	3 740
Коммутационный шнур с разъемами 110-110, 1 пара - 1,0 м	132	134	17 688
Монтажное оборудование	4	3 500	14 000
Шкаф напольный 42 U, 2033х800х875 мм	1	32 122	32 122
Комплект для соединения шкафов	1	7 222	7 222
Модуль вентиляторный 600 Series (монтаж сверху) - 2 вентилятора	1	4 700	4 700
Комплект для заземления	1	438	438
Полка перфорированная для оборудования 19" длиной 454 мм	1	1 030	1 030
Силовые розетки для шкафов, вертикальные, 8 розеток	2	2 160	4 320
Итого по офису г. *СЕВЕРНАЯ КВАНЗА* …			3.112.785
ВСЕГО ПО ПРОЕКТУ: 17 755 789			
Оплата разработки проекта			200 000
Сертификат на обучение персонала по эксплуатации сооружений связи	6	45 000	225 000
Итого по компании:			18 180 789

При приобретении оборудования были предусмотрены следующие статьи затрат: Кпр – затраты на приобретение оборудования 18 180 789 руб; Ктр – транспортные (в том числе таможенные) расходы расходы (4% от Кпр); Ксмр – строительно-монтажные расходы (20% от Кпр); Кт/у – расходы на тару и упаковку (0,5% от Кпр); Кзср – заготовительно-складские расходы (1,2% от Кпр); Кпнр – прочие непредвиденные расходы (3% от Кпр).

Расчет затрат на прокладку волоконно-оптического кабеля от здания офиса компании (от маршрутизатора VPN в серверной) до АТС (точки подключения к сети провайдера) зависит от длины кабельного сегмента. В проекте стоимость прокладки 1 км волоконно-оптического кабеля связи в канализации, с учетом монтажных и строительных работ (включая сварку, монтаж муфт, коннекторов, устройство вводов кабеля в здание, монтаж в шкафах и стойках, и др.) взята ориентировочной, с сайта компании-

подрядчика [28].

Общие затраты на прокладку кабеля составят:

$$K_{каб} = L * Y \quad (6.2)$$

где L – длина трассы прокладки кабеля, км; Y – стоимость 1 км прокладки кабеля в телефонной кабельной канализации.

В Луанде и остальных городах, где расположены офисы компании, средняя длина сегмента составляет порядка 1 км. Поэтому расчет затрат на строительсво сегмента ВОЛС сделан для всех 6 филиалов:

$$K_{каб} = L * Y = 6 * 80000 = 480000 \ руб$$

Таким образом, общие капитальные вложения рассчитываются как:

$$KB = K_{об} + (K_{пр} + K_{тр} + K_{смр} + K_{т/у} + K_{зср} + K_{пнр}) K_{об} + K_{каб}, \text{ руб} \quad (6.3)$$

$$KB = 18180\,789 + 18180\,789 * (0.04 + 0.2 + 0.03 + 0.012 + 0.005) + 480000 = 230878676 \text{ руб}$$

6 .2 Калькуляция эксплуатационных расходов

Эксплуатационными расходами называются текущие расходы предприятия на содержание и обслуживание сети.

Для определения эксплуатационных расходов по проекту используются следующие статьи:

1. затраты на оплату труда;
2. страховые взносы;
3. амортизация основных фондов;
4. материальные затраты;
5. прочие производственные расходы;

6. стоимость аренды VPN (150 000руб в месяц)
7. стоимость лицензии на оборудование

Состав персонала представлен в проекте в виде таблицы. Сумма оклада работника зависит от региона, где он работает, с учетом тарифной сетки в Анголе.

Таблица 6.2 – Состав персонала по обслуживанию оборудования

Наименование должности	Оклад	Количество, чел.	Сумма з/п, руб.
Ведущий инженер, начальник IT-отдела	200 000	1	200 000
Инженер 1 кат.	170 000	1	170 000
Инженер-программист	150 000	2	300 000
Монтажник	80 000	2	160 000
Итого:		6	830 000

Годовой фонд оплаты труда для персонала рассчитывается как:

$$ФОТ = \sum_{i=1}^{K} (T * P_i * I_i) * 12 \text{, руб} \quad (6.4)$$

где: I_i – количество работников каждой категории; P_i – заработная плата работника каждой категории, руб; 12 – количество месяцев: Т – коэффициент премии (если премии не предусмотрены, то Т=1).

ФОТ=830000*12=9960000

В случае, если необходимо ввести в штат сотрудников, которые будут заниматься строительством и прокладкой линейно-кабельных сооружений, то для них целесообразно составить отдельную таблицу.

Как видно, на сегодняшний день (2017 год) этот показатель составляет

порядка 30% от заработной платы. В случае, если доход работника за 1 год превысит 796 тыс. рублей, то на него вносится дополнительный налог в 10%.При превышении базы в 718 тыс. рублей взносы в ФСС не уплачиваются).

$$СВ = ФОТ * 0{,}4 \text{, руб} \qquad (6.5)$$

Под амортизацией понимается процесс постепенного возмещения стоимости основных фондов, в целях накопления средств для реконструкции и приобретения основных средств:

$$СВ=9960000*0{,}4=3984000$$

$$AO = T / F = 17.755.789/10 = 1775578 \text{, руб} \qquad (6.6)$$

где Т – стоимость оборудования,

F – срок службы этого оборудования.

Величина материальных затрат включает в себя оплату электроэнергии для производственных нужд, затраты на материалы и запасные части и др. Эти составляющие материальных затрат определяются следующим образом:

а) затраты на оплату электроэнергии определяются в зависимости от мощности станционного оборудования:

$$З_{эн} = T * 24 * 365 * P \qquad (6.7)$$

где Т – тариф на электроэнергию (руб./кВт · час), Р – мощность установок (кВт).

где Т = 4,5 руб/кВт час – тариф на электроэнергию.

P =45 кВт – мощность установок

Тогда, затраты на электроэнергию составят

$$З_{эн} = 4{,}5 * 8760 * 45 = 1773900$$

Стоимость кВт выбирается в зависимости от конкретного региона, в котором планируется строительство сети, цены для Республики Ангола «Министерство энергии и воды» по электронному адресу http://www.minea.gv.ao/

б) затраты на материалы и запасные части составляют 3,5% от основных производственных фондов и определяются по формуле:

$$З_{мз} = КВ * 0{,}035 \quad (6.8)$$

где КВ – капитальные вложения, затраты на оборудование.

Общие материальные затраты равны: **17.755.789*0,035=621453**

$$З_{общ} = З_{эн} + З_{мз} \quad (6.9)$$

где $З_{эн}$ – затраты на оплату электроэнергии; $З_{м}$ – материальные затраты.

Прочие расходы предусматривают общие производственные ($З_{пр.}$) и эксплуатационно-хозяйственные затраты ($З_{эк.}$):

$$З_{пр} = ФОТ * 0{,}1 \quad (6.10)$$

$$З_{эк} = ФОТ * 0{,}1 \quad (6.11)$$

где ФОТ – годовой фонд оплаты труда.

Отчисления на научно-исследовательские и опытно-конструкторские работы (НИОКР) составляют 1,5% от всей суммы эксплуатационных расходов (если таковые предусмотрены).

Результаты расчета годовых эксплуатационных расчетов сводятся в общую таблицу (таблица 6.3)

Таблица 6.3 – Годовые эксплуатационные расходы

Наименование затрат	Сумма затрат, руб.	Удельный вес статей, %
1. ФОТ	9960000	0,529473
2. Страховые взносы	3984000	0,211789
3. Амортизационные отчисления	1681780	0,089403
4. Материальные затраты	588595	0,03129
5. Прочие расходы	796800	0,042358
6. Аренда VPN	1800000	0,095688
7. Лицензия для маршрутизатора Cisco 2811/K9: VPN с поддержкой безопасности и шифрования (VPN сервер + VPN клиент, до 10 клиентов)	50 985	0,002710357
ИТОГО	18862160	100

Выводы по разделу

Осуществлена оценка капитальных вложений в предлагаемый проект и калькуляция эксплуатационных расходов. Рассчитанные технико-экономические показатели сведены в таблицу 6.4.

Таблица 6.4 – Основные технико-экономические показатели проекта

Показатели	**Численные значения**
Количество абонентов, чел	**1464**
Капитальные затраты, руб	**23 087 676**
Ежегодные эксплуатационные расходы, руб, в том числе:	**18 862 160**
ФОТ	9960000
Страховые взносы	3984000
Амортизационные отчисления	1681780
Материальные затраты	588595
Прочие расходы	796800
Аренда VPN	1800000
Лицензия для маршрутизатора Cisco 2811/K9: VPN с поддержкой безопасности и шифрования (VPN сервер + VPN клиент, до 10 клиентов)	50 985

На реализацию проекта потребуется **23 0871 676** руб. Сумма годовых эксплуатационных расходов составит 18 862 160 руб. с учетом ежегодных отчислений на аренду VPN у провайдера Ангола Телеком, и затрат на продление лицензии. [24]

ЗАКЛЮЧЕНИЕ

В выпускной квалификационной работе представлено возможное решение по созданию инфокоммуникационной инфраструктуры группы компаний Odebrecht в Республике Ангола.

Анализ инфраструктуры показал, что сотрудники ГК Odebrecht республики Ангола не имеют возможности использования высококачественных телекоммуникационных сервисов. Для решения этой задачи выбраны варианты реализации сетей связи в офисах компании, и разработана транспортная инфраструктура на основе VPN.

Для удовлетворения потребностей пользователей в получении телекоммуникационных услуг целесообразно использовать технологию Ethernet и реализовать сеть связи в филиалах на основе мультисервисной платформы IP PBX Cisco Business Edition 6000, которая представляет собой оборудование для передачи голосового трафика и трафика данных в пакетном режиме. Для реализации механизмов VPN выбраны маршрутизаторы Cisco линейки 2800, на основе которых реализован сетевой сегмент, являющийся пограничным шлюзом VPN и одновременно устройством, контролирующим и управляющим передачей данных в подсетях филиалов. Для обеспечения безопасности и возможности шифрования трафика предусмотрено приобретение дополнительной лицензии, при этом в центральном офисе г.Луанда маршрутизатор будет являться VPN-сервером, а в филиалах – VPN-клиентом, что позволяет приобрести не 6 лицензий, а одну, и приведет к экономии средств компании. Для безопасного доступа в сеть Интернет будет использован Межсетевой экран CISCO ASA5505-K8 ASA 5505 Appliance with SW. Для организации работы серверов также было выбрано решение на базе оборудования Cisco Серверная платформа Cisco Unified Computing System UCSC-C240-M4S. Несмотря на высокую стоимость оборудования данного производителя,

реализация проектного решения позволит добиться таких показателей, как надежность, легкая настройка и конфигурирование сетевых сегментов, а также обеспечит экономию средств на подготовку специалистов.

Экономическая оценка проекта позволила оценить требуемы вложения, капитальные вложения составили 23 331 700 рублей, эксплуатационные расходы – 18 862 160 рублей.

Таким образом, спроектирована территориально-распределённая сеть связи для 1464 абонентов, с учётом возможности взаимодействия 6 филиалов друг с другом и оптимизации затрат на услуги связи.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ODEBRECTH 2015 Annual Report Sustainability results [Электронный ресурс] /Режим доступа - http://www.odebrecht.com – официальный сайт компании ODEBRECTH (дата обращения 01.03.2017)

2. RUSTELECOM Catalog Ethernet [Электронный ресурс]/ Режим доступа http://www.rus-telcom.ru/catalog/Ethernet/Ethernet-com-2.html (дата обращения 03.03.2017)

3. JUST NETWORKS 2017 [Электронный ресурс] Режим доступа / http://just-networks.ru/lokalnye-vychislitelnye-seti/tekhnologiya-ethernet (дата обращения 03.03.2017)

4. JUSTGROUP.RU 2017. [Электронный ресурс] Режим доступа / http://www.justogroup.ru/cisco/router/2900-series/cisco2901_k9 (дата обращения 03.03.2017)

5. Денисова, Т.Б. Построение виртуальной частной сети. Методическое пособие для курсового и дипломного проектирования. - ПГАТИ. – Самара, 2006 [Электронный ресурс]/ Режим доступа: www.msib.psuti.ru›content/metod/Денисова_ КП VPN.pdf Дата обращения (04.03.2017)

6. Сердюк, В.А. Организация и технологии защиты информации. Обнаружение предотвращение информационных атак в автоматизированных системах предприятий / В.А. Сердюк. - М. : НИУ Высшая школа экономики, 2011 [Электронныйресурс]/ Режим доступа http://biblioclub.ru/index. php?page=book&id=74298 (дата обращения 05.03.2017)

7. Обработка и обеспечение безопасности электронных данных : учебное пособие / А.В. Агапов, Т.В. Алексеева, А.В. Васильев и др. ; под общ. ред. Д.В. Денисов. - М.: Московский финансово-промышленный университет «Синергия», 2012. [Электронный ресурс]/ Режим доступа: http://biblioclub.ru/index.php?page=book&id=252894 (дата обращения

07.03.2017)

8. MOB-MOBILE.ip telephone [Электронный ресурс]/ Режим доступа http://mob-mobile.ru/statya/4676-ip-telefon-chto-eto-takoe-i-zachem-nuzhen.html (дата обращения 09.03.2017)

9. NAG RU technology [Электронный ресурс]/ Режим доступа https://shop.nag.ru/article/o-kompanii/. (дата обращения 09.03.2017)

10. NESTORE Cisco CISCO2811-SEC/K9 2811 Security BundleAdv Security128F/512D [Электронный ресурс]/ Режим доступа https://netstore.su/katalog/cetevoe-oborudovanie-1430772915/marshrutizatori-1012331714/marshrutizatori-cisco/marshrutizatori-cisco-2800/cisco2811-sec_k9 (дата обращения 11.03.2017)

11. Cisco Business Edition 6000 Solutions Data Sheet [Электронный ресурс]/ Режим доступа: http://www.cisco.com/c/ru_ru/products/unified-communications/business-edition-6000/index.html (дата обращения 12.04.2017г)

12. Телекоммуникационные системы и сети: учебное пособие. В 3 томах. Том 2 - Радиосвязь, радиовещание, телевидение / Катунин Г.П., Мамчев Г.В. и др. - М.: Горячая линия-Телеком, 2004. - 672 с. (дата обращения 14.03.2017)

13. Волоконно-оптический кабель длявнешней прокладки в соответствии с DIN VDE 0888 марки A-DQ(ZN)B2Y [Электронный ресурс]/ Режимдоступаhttp://www.telcomtrade.ru/upload/image/products/pdf/1DB_80196_ru.pdf (дата обращения 16.03.2017)

14. Телеком-Трейд: Кабельная продукция от ведущих европейских производителей [Электронный ресурс]/ Режим доступа: http://www.telcomtrade.ru/catalog/Helukabel/volokno/h_a_dqznb2y_central/ (дата обращения 10.03.2017)

15. Сетевое оборудование оптом [Электронный ресурс] // Официальный сайт компании NetCom Е.: Режим доступа www.netcom.ru

(дата обращения 20.03.15)

16. IP-УАТС Panasonic KX-NS1000 RU [Электронный ресурс]/ Режим доступа: http://i2000.ru/ishop/4308/27630 (дата обращения 21.03.2017).

17. Протоколы интернета [Электронный ресурс]: Режим доступа http://tibanews.com/ss/tibanet/index.php/ip/ip-basic/types-ip. (дата обращения 18.03.2017).

18. Каталог оборудования Интернет и Телефония АТС CISCO [Электронный ресурс]/ Режим доступа http://www.ntel.ru/equipment-catalog/internet-n-telephony/ats/cisco/data/79/ (дата обращения 30.03.2017).

19. DHCP (Dynamic Host Configuration Protocol). [Электронный ресурс]Режимдоступаhttp://www.idconline.com/technical_references/pdfs/data_communications/DHCP.pdf. Дата обращения (30.05.2017).

20. OSK GROUP [Электронный ресурс] // Официальный сайт компании// Режим доступа http://optiksk.ru/opticheka belmoskabelfudzhura/ vnutriobektovye/modulnyj-oktm-n.html// Дата обращения (05.05.2017)

22. Компания Оптические технологии: SVARKA-OPTIKI [Электронный ресурс]// Режим доступа http://svarka-optiki.ru/index.php, (дата обращения 03.06.2017)

23. Стоимость монтажных работ (ALL-LINES) [Электронный ресурс] Режим доступа http://www.all-lines.ru/bystryj-raschet - компания All-lines http://www.nta.ru/site/service/rashet.html, http://vols.su/?page_id=6)
(дата обращения 31.05.2017)

24. Болдышев А.В. Методические рекомендации по выполнению технико-экономического обоснования выпускных квалификационных работ. [Электронный ресурс] / http://knit.bsu.edu.ru/knit - сайт Факультета информационных технологий и прикладной математики. Режим доступа http://knit.bsu.edu.ru/knit/resources/docs.php (дата обращения 30.05.2017)

25. Цена IP PBX Cisco [Электронный ресурс]/ Режим доступа

http://www.open-vision.ru Системный интегратор Open Vision//http://www.open-vision.ru/about/actions/archive/cisco-be-6000-sale/ (дата обращения 25.04.2017г)

26. Межсетевой экран CISCO ASA5505-K8 ASA 5505 Appliance with SW [Электронный ресурс]/ http: Режим доступа www.ediscom.ru - Discom Network Technologie Системный интегратор // URL: http://www.ediscom.ru/catalog/cisco_5/mezhsetevoy_ekran_cisco_asa5505_k8_asa_5505_appliance_with_sw_10_users_8_ports/?utm_source=yandex&utm_medium=cpc&utm_campaign=12954112&utm_content=1718712782&utm_term=ASA5505- K8&region=4&region_name=%d0%91%d0%b5%d0%bb%d0%b3%d0%be%d1%80%d0%be%d0%b4&block=premium&position=2&_openstat=ZGlyZWN0LnlhbmRleC5ydTsxMjk1NDExMjsxNzE4NzEyNzgyO3lhbmRleC5ydTpwcmVtaXVt&yclid=3405866434125894528 (дата обращения 26.04.2017г)

27. Лагунцов Е. Технологии Cisco для построения эффективного ЦОД, на базе решения FlexPod/ Серверная платформа Cisco Unified Computing System [Электронный ресурс]/ Режим доступа: http://www.flane.ru/medi_a/pdf/UCS-Flexpod.pdf (дата обращения 27.04.2017г).

28. Базовые тарифы на ПИР и СМР [Электронный ресурс]/ http://www.voks-it.ru – сайт компании-подрядчика ООО «ВОКС ИТ»// Режим доступа:http://www.voksit.ru/index.php?option=com_content&view=article&id=64&Itemid=71 (дата обращения 31.05.2017г)

30. Калькулятор СКС [Электронный ресурс]/ Режим доступа: http://bitwifi.ru/produkty/wi-fi-infrastruktura/proektirovanie-wi-fi-seti-old/montazh-sks/work-calculator/ (дата обращения 03.05.2017).